2011

An Empirical Investigation of the Relationship between Computer Self-Efficacy and Information Privacy Concerns

Mohammad Abdul Awwal
Nova Southeastern University, mawwal323@hotmail.com

An Empirical Investigation of the Relationship between Computer Self-Efficacy and Information Privacy Concerns

By

Mohammad A. Awwal

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

Graduate School of Computer and Information Sciences
Nova Southeastern University

2010

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

---------- ----------

William L. Hafner, Ph.D. Date
Chairperson of Dissertation Committee

---------- ----------

Maxine S. Cohen, Ph.D. Date
Dissertation Committee Member

---------- ----------

Gurvirender P. Tejay, Ph.D. Date
Dissertation Committee Member

Approved:

---------- ----------

Leonidas Irakliots, Ph.D. Date
Dean

Graduate School of Computer and Information Sciences
Nova Southeastern University

2010

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

An Empirical Investigation of the Relationship between Computer Self-Efficacy and Information Privacy Concerns

by
Mohammad A. Awwal

December 2010

The Internet and the growth of Information Technology (IT) and their enhanced capabilities to collect personal information have given rise to many privacy issues. Unauthorized access of personal information may result in identity theft, stalking, harassment, and other invasions of privacy. Information privacy concerns are impediments to broad-scale adoption of the Internet for purchasing decisions. Computer self-efficacy has been shown to be an effective predictor of behavioral intention and a critical determinant of intention to use Information Technology. This study investigated the relationship between an individual's computer self-efficacy and information privacy concerns; and also examined the differences among different age groups and between genders regarding information privacy concerns and their relationships with computer self-efficacy.

A paper-based survey was designed to empirically assess computer self-efficacy and information privacy concerns. The survey was developed by combining existing validated scales for computer self-efficacy and information privacy concerns. The target population of this study was the residents of New Jersey, U.S.A. The assessment was done by using the mall-intercept approach in which individuals were asked to fill out the survey. The sample size for this study was 400 students, professionals, and mature adults.

The Shapiro-Wilk test was used for testing data normality and the Spearman rank-order test was used for correlation analyses. MANOVA test was used for comparing mean values of computer self-efficacy and information privacy concerns between genders and among age groups. The results showed that the correlation between computer self-efficacy and information privacy concerns was significant and positive; and there were differences between genders and among age groups regarding information privacy concerns and their relationships with computer self-efficacy.

This study contributed to the body of knowledge about the relationships among antecedents and consequences of information privacy concerns and computer self-efficacy. The findings of this study can help corporations to improve e-commerce by targeting privacy policy-making efforts to address the explicit areas of consumer privacy concerns. The results of this study can also help IT practitioners to develop privacy protection tools and processes to address specific consumer privacy concerns.

Acknowledgements

Dissertation process is a time consuming undertaking which requires dedication, sacrifice and support from friends, family members, adviser, and dissertation committee members. Therefore, I would like to thank those who held my hands and helped me to complete this long and difficult journey. Foremost gratitude is owed to my adviser Dr. William Hafner for his assistance and valuable feedbacks throughout the program. Additionally, I would like to thank my committee members, Dr. Maxine Cohen and Dr. Gurvirender Tejay for their guidance and helpful suggestions.

I would also like to acknowledge those who helped me through the process outside the university. I want to thank my beloved wife Afroza Awwal for her sacrifice, understanding, and support of my dream. My special thank to my younger son, Tanim Awwal, who has always provided moral support throughout the process. I want to thank my friends Dr. Wahiduzzaman, Dr. Afzal Hossain, Masroor Ahmed, and Burhan Mahmood for their inspirations and guidance.

Finally, I would like to thank everyone who participated in the survey process for their helpful inputs.

Table of Contents

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Statement of the Problem

The purpose of this dissertation was to investigate the relationship between an individual's computer self-efficacy and information privacy concerns; and also to investigate the differences among different age groups and between genders regarding information privacy concerns and their relationships with computer self-efficacy. Computer self-efficacy has been shown to be an effective predictor of behavioral intention (Ball, 2008) and a critical predictor of an individual's attitude about information technology and usage behaviors (Marakas, Yi, & Johnson, 1998). Consumers' privacy concerns are complex and practitioners and researchers need to understand antecedents to consumers' concerns regarding information privacy (Stewart & Segars, 2002). Several studies (Malhotra, Kim, & Agarwal, 2004; Metzger, 2004; Phelps, Nowak, & Ferrel, 2000; Anton, Earp, He, Stufflebam, Bolchini, & Jensen, 2004) have shown that if consumers' privacy concerns are not understood and mitigated, they can have negative consequences on e-commerce growth and Internet purchases. White, Shah, Cook, and Mendez (2008) studied the relationship between computer self-efficacy and information privacy concerns. Their study focused on computer self-efficacy and its relationship with the four information privacy components (collection of data, errors (data integrity), unauthorized secondary use, and improper access to data) as defined by Smith, Milberg,

and Burke (1996). They used two measuring instruments: 1) Concern for Information Privacy (CFIP), developed by Smith et al. (1996) and 2) The Computer Self-Efficacy scale (CSES) developed by Murphy, Coover, and Owen (1989). White et al. (2008) used old measuring scales (CFIP in 1996 and CSES in 1989) for their study. CFIP measures the privacy concerns of an organization's practice of managing personal information (Stewart & Segars, 2002) and does not address privacy concerns for Internet users (Malhotra et al., 2004). CSES measure was developed in 1989 and focused on mainframe skills and does not measure computer self-efficacy of today's computing technology like windows, spreadsheet, database, and Internet. The study sample of White et al. (2008) consisted of young undergraduate students only and did not include professionals and mature adults. They also did not study the differences of relationships between information privacy concerns and computer self-efficacy among different age groups and genders. Their results lack external validity and cannot be generalized due to their study population (students only). Zukowski and Brown (2007) found that older Internet users were more concerned about information privacy than younger users. Sheehan (1999) found that women were more concerned about information privacy than men. White et al. (2008) stressed the need to extend their work with a broader population and also to examine the differences of the relationships among different age groups and between genders. They also emphasized the need to validate their work with updated measuring scales to reflect current technology. Many researchers (Stewart & Segars, 2002; Marakas, Johnson, & Clay, 2007) stated that measuring scales might not be valid over time and measuring scales must evolve to reflect changes in computer technology. Stewart and Segars (2002) argued that CFIP should be reinvestigated in light of emerging technology.

Old scales may not measure computer self-efficacy and information privacy concerns accurately to reflect today's technology and therefore the results may lack internal validity.

Research Goals

The main goal of this study was to validate the work of White et al. (2008) by investigating their findings with a broader population and with updated measuring scales; and to extend their work by investigating differences among different age groups and between genders regarding information privacy concerns and their relationships with computer self-efficacy. The first specific goal of this study was to empirically investigate relationship between computer self-efficacy (CSE) and information privacy concerns (IPC) with a broader population (different age groups and genders) and with updated measuring scales to reflect current technology. The second specific goal of this study was to investigate correlation differences between CSE and IPC among different age groups. The third specific goal of this study was to investigate correlation differences between CSE and IPC between genders (male and female). For assessing information privacy concerns (IPC), the three-dimensional (*collection, control, awareness*) measuring scale of the Internet Users' Information Privacy Concerns (IUIPC), developed by Malhotra et al. (2004) was used. This was an updated CFIP scale with an additional dimension (awareness) to measure privacy concerns of Internet users. For assessing computer self-efficacy (CSE), six-dimensional (*general computer efficacy, windows computer efficacy, spreadsheet use efficacy, word processing efficacy, Internet efficacy, and database efficacy*) measuring scale of the Computer Self-Efficacy Scale (CSES), developed by

Marakas et al. (2007) was used. The CSES adhered to the base theory of general computing and they were also in keeping with the current state of computer technology (windows computer use, spreadsheet use, word processing skills, internet skills, and database skills).

Research Questions

This dissertation was built on previous research (White et al., 2008; Malhotra et al, 2004; Marakas et al., 2007) by investigating the relationship between computer self-efficacy (CSE) and information privacy concerns (IPC). The IPC was a *dependent variable* and the CSE was an *independent variab*le for this study. The age groups and genders were the *moderator variables* for this study. Figure 1 shows the research model depicting this relationship. The two research questions that this study addressed were:

1. Is there a relationship between an individual's information privacy concerns and her computer self-efficacy?
2. Is there any difference among different age groups (18-25, 26-50, 50+) and between genders with respect to their relationship between computer self-efficacy and information privacy concerns?

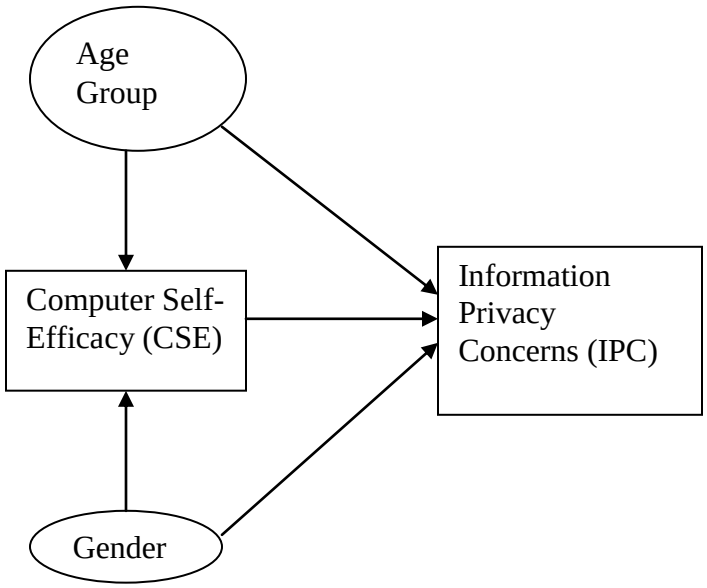

Figure 1. Research model depicting the relationship among computer self-efficacy, age groups, gender, and information privacy concerns.

Research Hypotheses

In seeking answers to the research questions, five null hypotheses were used. Research question one was addressed by hypothesis one and research question two was addressed by hypotheses two, three, four and five. The five null hypotheses are as follows:

H_{01}: There is not a significant relationship between an individual's concern for information privacy and her computer self-efficacy.

H_{02}: There is not a significant relationship between information privacy concerns and age groups.

H_{03}: There is not a significant relationship between information privacy concerns and gender.

H_{04}: There is not a significant relationship between computer self-efficacy and age groups.

H_{05}: There is not a significant relationship between computer self-efficacy and gender.

Relevance and Significance of the Study

Relevance of the Study

The growth of Information Technology and its enhanced capability to collect personal information have given rise to privacy issues (Mason, 1986). The consumers are concerned that their personal information will be used for purposes other than those for which it was collected (Turner & Dasgupta, 2003). Pollach (2006) found that users' privacy concerns were well founded and most of the companies through their privacy policy statements admitted to the very practices (data collection and data sharing) about which consumers were concerned. The winning companies in electronic commerce will be those who understand and respond to consumers' privacy concerns (Luo & Seyedian, 2004).

Many researchers (Zukowski & Brown, 2007; O'Neil, 2001; Sheehan, 1999) investigated relationships between privacy concerns and various demographic factors (age, gender, income level, and education). Little published research exists that relates an individual's computer self-efficacy with information privacy concerns. To date, there is only one study (White et al., 2008) which examined relationship between information privacy concern and computer self-efficacy. White et al. (2008) used undergraduate students only in their study; and therefore, their results cannot be generalized. The

relevance of this study was that by relating computer self-efficacy to information privacy concerns , this research filled the gap in the academic literature as the public's, nonprofit and private sectors' and governments' interest in information privacy continued to grow.

Significance of the Study

This research extended the work of White et al. (2008) by validating their results with a broader population (different age groups and genders) and with updated measuring scales to reflect Internet and current technology. Additionally, this study also investigated the correlation differences between information privacy concerns and computer self-efficacy among different age groups and between genders. The results of this study can help corporations to improve e-commerce by targeting privacy policy-making efforts to address the explicit areas of consumers' privacy concerns. For researchers, this study addressed the relationships among the antecedents and consequences of information privacy concern and computer self-efficacy.

Limitations and Delimitation of the Study

Limitations of the Study

There were three limitations in this study. The first limitation of this study related to the external validity of results. This study used the mall-intercept method (Stewart & Segars, 2002) in shopping centers and college campuses. Although, attempts were made to include participants from various backgrounds of job functions, different age groups, and different educational backgrounds, participants might not represent general population. Further studies will be needed to validate the findings with different users in different contexts. The second limitation was generalization. The target population for

this study was the residents of New Jersey, U.S.A. While a large enough sample might be generalized to the target area, the rest of the U.S.A might not be represented. Further studies will be needed with users from other states to generalize the findings. The third limitation of this study was that the measuring scale of information privacy concerns which did not include items to measure concerns for identity theft and data security. Further study will be required with an updated scale that will include items to measure concerns for identity theft and data security.

Delimitation of the Study

There were several delimitations in this study. The first was the sample size to improve generalization in each age group (18-25, 26-50, and 50+) and in each gender (male and female). Since the survey for this research was conducted in person, the sample size was controlled by the researcher. However, since the researcher was soliciting subjects through convenience, solicited subjects might not represent entire population of the state. This study used a convenience sample and limited the participants to the residents of one state only. The second delimitation of this study was information privacy concern dimensions. This research investigated relationship between computer self-efficacy and information privacy concerns with three dimensions (collection, control, and awareness) which were defined by Malhotra et al. (2004). The collection measured the consumers' privacy concern of organization's practice of collecting personal information. The control measured privacy concerns related to consumers' right to exercise control and autonomy over decisions about how their information was collected, used, and shared. The awareness measured consumers' privacy concerns related to awareness and knowledge about of how their personal information was used. These dimensions did not

address privacy concerns related to security and protection of personal information. The third delimitation was the measuring instruments. This study used an updated IUIPC scale (Malhotra et al, 2004) and an updated CSE scale (Marakas et al., 2007) which reflected today's technology. Marakas et al. (1998) reported that instrument validation was an ongoing process and measuring instruments needed to be updated over time with shift of technology.

Barriers and Issues

The populations of the majority of the studies (Murphy et al., 1989; Liang, 2005; Marakas et al., 2007; Hill et al., 1987; Buchanan et al., 2007) were university students who were easily accessible and responded to classroom surveys. Professionals and mature adults are busy and do not normally respond to email or Internet surveys. That is why, in earlier research, the goal of this research to investigate with a broader population has not been achieved. By conducting surveys in person face-to-face with students, professionals, and mature adults in various places like indoor shopping areas, government buildings, coffee shops, colleges, and market areas, the goal of this research was achieved.

Definition of Terms

Behavioral Intention (BI) – A measure of the strength of one's intention to perform a specified behavior (Blanke, 2008).

Compute Self-Efficacy (CSE) – One's ability to apply his or her computer skills to a wide range of tasks (Compeau & Higgins, 1995).

Concern for Information Privacy (CFIP) – a 15-item information privacy concern measuring scale, with four dimensions (collection, errors, secondary use, and unauthorized access), which was developed by Smith et al. (1996).

Cryptography – A mathematical algorithm of encoding messages so that original messages are indecipherable and decoding messages so that original messages can be understood (Kuechler & Grupe, 2003).

Digital Economy – "Refers to an economy that is based on digital technologies. The digital economy is also sometimes called the Internet economy, the new economy, or the Web economy" (Turban, Leidner, Mclean, & Wetherbe, 2008).

E-Commerce – "Electronic commerce (EC or E-Commerce) describes the process of buying, selling, transferring, or exchanging products, services, or information via computer networks, including the Internet (Turban, Leidner, Mclean, & Wetherbe, 2008). "Conducting trade for products and services between organizations or an organization and individuals via digitally enabled transactions over the Internet" (King, 2008, p.11).

E-Business – "Refers to a broader definition of EC, not just the buying and selling of goods and services, but also servicing customers, collaborating with business partners, conducting electronic transactions within an organization" (Turban et al., 2008).

General Computer Self-Efficacy (GCSE) – An individual's judgment of efficacy across multiple computer application domains (Marakas et al., 1998).

Information Privacy – An individual's ability to control the collection and use of personal information (Westin, 1967).

Internet Users' Information Privacy Concerns (IUIPC) – A 10-item information privacy concern measuring scale for Internet users, with three dimensions (collection, controls, and awareness), which was developed by Malhotra et al. (2004).

Personal Information – Information that identifies an individual (Culnan & Armstrong, 1999).

Personalization – "The ability to provide content and services that are tailored to individuals based on knowledge about their preferences and behaviors" (Adomavicius & Tuzhilin, 2005, p. 84).

Privacy – "The moral right of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state" (Laudon & Traver, 2001, p.467).

Privacy Concerns – People's concerns about the control of their personal information (Sheng, Nah, & Siau, 2008).

Self-Efficacy (SE) – People's judgment of their capabilities to organize and execute courses of action required to perform a task (Bandura, 1986).

Social Learning Theory (SLT) – It is also called Bandura's (1986) Social Cognitive Theory (SCT). The theory states that psychological procedures alter the level and strength of self-efficacy and expectation of personal efficacy are derived from four principal sources of information: performance accomplishments, vicarious experience, verbal persuasion, and physiological states (Bandura, 1977).

Technology Acceptance Model (TAM) – Classical information system model which is developed to explain computer-usage behavior and constructs associated with acceptance of technology (Davis, 1986).

Summary

This study investigated the relationship between an individual's computer self-efficacy and her information privacy concerns. A conceptual research model depicting this relationship is shown in Figure 1. Two research questions were formulated to address research problem and five null hypotheses were defined to seek answers to the research questions. The main goal of this study was to empirically validate the research model using students', professionals', and mature adults' computer self-efficacy and information privacy concerns.

The relevance of this study stemmed from the need for understanding all antecedents to information privacy concerns as the publics', nonprofit and private sectors', and governments' interest in information privacy continued to grow.

The significance of this study was demonstrated by validating the work of White et al. (2008) with a broader population and with updated measuring scales that reflected Internet and current technology. The results of this study can help corporations to improve e-commerce by targeting privacy policy-making efforts to address the explicit areas of consumers' privacy concerns.

Chapter 2

Review of the Literature

Introduction

With the growth of enhanced capabilities of Internet and other information technologies to collect personal information, consumers are concerned about their privacy (Pollach, 2006; Mason, 1986). This study investigated the relationship between an individual's computer self-efficacy (independent variable) and her information privacy concerns (dependent variable). There were four main areas relevant to this study. They were information privacy concerns, privacy measuring instruments, computer self-efficacy, and computer self-efficacy measuring instruments. The discussion proceeded with the summary of what was known and unknown about the topic.

Privacy Concerns

"Privacy is and will always be important to people" (Nakos, 2003, p. 2). With the growth of Internet usage, privacy concern is on the rise and wide spread (Nakos, 2003). Information privacy refers to an individual's ability to control the collection and use of personal information (Westin, 1967; Stone, Gardner, Gueutal, & McClure, 1983). Westin (1967) proposed a privacy topology and categorized individual's privacy concerns into three groups: privacy *fundamentalists*, privacy *unconcerned*, and privacy *pragmatists*. The privacy fundamentalists are extremely concerned about their personal information

and they are unwilling to provide their personal information. Individuals in the privacy unconcerned group are not concerned about their privacy and they are willing to provide their personal information. The privacy pragmatists are more concerned about their privacy than privacy fundamentalists.

Personal information is information that identifies an individual (Culnan & Armstrong, 1999). There is a growing concern about how much individuals can control the collection and use of their personal information (Phelps, Nowak, & Ferrel, 2000; Stewart & Segars, 2002). Privacy is a major concern in web-based applications and the lack of consumer confidence in information privacy has been identified as a major problem for the growth of E-commerce (Zviran, 2008; Malhotra et al., 2004). The review of literature specific to information privacy concerns was performed in the context of collection, control, and awareness of personal information. The literature review also included studies related to antecedents to information privacy concerns in the context of age, gender, and computer self-efficacy. The studies specific to information privacy concerns can be grouped into three main areas: privacy concerns in direct marketing, privacy concerns in E-commerce, and antecedents to privacy concerns.

Privacy Concerns in Direct Marketing

Direct marketers (telemarketers) contact individuals by direct mail, e-mail, or telephone and require them to respond to make a purchase (Turban et al., 2008). Websites collect personal information which enables them to mass email solicitations and target both their own and others' advertisings to consumers (Pippin, 1999). Marketers have built and will continue to build databases with consumers' personal information and will use this information to target and profile consumers (Milne & Rohm, 2000). Consumers are

concerned with privacy and protection of their personal information collected by the direct marketers (Culnan, 1995; Phelps, Nowak, & Ferrel, 2000; Stewart & Segars, 2002).

Smith, Milberg, and Burke (1996) identified four dimensions of privacy concerns (collection, errors, secondary use, and unauthorized access) with respect to organizations management of personal data. They found that consumers were concerned that: too much data was collected by marketers, much of the data was inaccurate, their personal information could be used for undisclosed purposes, and corporation could not protect their personal information.

Culnan (1995) studied consumers' awareness of name removal procedure from mailing list and found consumers, who were aware of name removal procedure from direct marketers' mailing list, were more concerned about privacy than those who were unaware of name removal procedure. Her study focused on the use of secondary information – information that was collected for one purpose, was reused for another purpose by the firms. The results also showed that consumers, who were unaware of name removal procedures, tended to be young, poor, and less educated African-American mail shoppers; and they were less likely to be concerned about privacy than consumers who were aware of name removal procedures.

Milne and Rohm (2000) examined consumer perspective of data collection awareness and knowledge of name removal mechanism, such as opt in and opt out, across mail, email, telephone, and Internet direct channels. The results showed that consumers were neither aware of data collection efforts by the marketers nor knowledgeable of name removal mechanisms. The results also showed that consumers were most likely to desire

removal of their names from telephone list compared with email or mail list and they preferred alternative formats and notification schedule over standard opt-out procedures.

Phelps, Nowak, and Ferrel (2000) found that consumers were very concerned with collection of personal information. The consumers believed that there should be limits on how much information companies could collect, companies should not share mailing list with other companies, and companies should remove their names from mailing and telephone lists. Phelps et al.(2000) examined consumers' privacy concern-behavior consistency and their perceptions regarding the exchange relationship with direct marketers who gather and use personal information; and they found six factors of privacy concerns: 1) type of personal information requested, 2) consumers' ability and desire to control dissemination of personal information, 3) consumers' perceptions regarding marketers' knowledge about them and their interests, 4) consumers' attitude toward direct mails, 5) consumers' preferences with respect to catalog and advertising mail volume, and 6) previous name removal request.

Phelps, D'Souza, and Nowak (2001) examined the relationship between antecedents and consequences of privacy concerns in the context of direct marketing. The results showed that the consumers' attitude toward direct marketing and their desire for control over their personal information acted as antecedents to privacy concerns; and as privacy concerns increased, purchase behavior decreased.

Stewart and Segars (2002) found that privacy concerns were multi-dimensional with respect to direct marketing. They examined four dimensions of information privacy concerns (collection, errors, secondary use, and unauthorized access) posited by Smith et al. (1996) and found that the consumers were concerned about all four dimensions.

Dolnicar and Jordaan (2007) found that consumers were concerned about the control of their personal information collected by the marketers. They conducted two empirical studies in two countries (South Africa and Australia) to investigate consumers' views on information privacy concerns related to direct marketing activities. The results showed that significant privacy-related concerns existed among consumers of both the countries and privacy concerns were associated with both actively protective behaviors (requesting deletion of personal information from the company's database) and passively protective behaviors (avoiding shopping over telephone).

Milne and Rohm (2000) found that as marketers continued to build databases with consumer information, they often traded and rented this information to other organizations; and consumers concerns continued to grow

Privacy Concerns in E-Commerce

In digital economy, E-commerce refers to the process of buying, selling, transferring, serving, or exchanging products, services, or information via computer networks, including the Internet (Turban et al., 2008). The Internet has changed the global economy (Graubert & Coleman, 1999; Pippin, 1999). Consumer privacy issue is a complicated issue and the Internet has made it more difficult (Pippin, 1999). The Internet's unprecedented potential for data collection and data sharing, and lack of consumers' awareness and control of their personal information collected by the Internet firms have increased consumers' privacy concerns; and information privacy concerns have become a central issue in electronic commerce and consumer-oriented use of the Internet (Garfinkel, 2000; Kelly, 2000; Miyazaki & Fernandez, 2000). For companies and organizations, the Internet represents the promise of better, cheaper, and efficient

marketing (Richards, 1997). However, consumers are increasingly concerned about how their personal information is being used (Muris, 2001; Phelps et al., 2000); and they have no control on how much data is collected (Dhillon & Moores, 2001; Chen & Rea, 2004).

According to Graubert and Coleman (1999), since the Internet is global in nature, the issue of privacy protection has an international dimension. The United States and European Union have developed various privacy laws to protect collection, flow, and retention of personal information. The United States has relied primarily on self-regulatory approach to protect personal information. They found that while the government involvement and self-regulatory programs were necessary to address the privacy concerns, the most effective way to protect the privacy of online users might ultimately come from the high-tech marketplace itself.

According to Pippin (1999), the Internet is an under-regulated commercial tool which is also a medium where a huge volume of personal information is stored; and that can be accessed by anyone. Pippin also found that privacy laws in the United States mainly targeted specific industries that collected personal data; and no law covered all consumers in the collection of personal data on-line. He suggested that consumers should be encouraged to protect themselves on-line through education.

Sheehan and Hoy (1999) investigated the relationship between the consumers' privacy concerns and their behavior in an online environment. The results showed that there was a significant relationship between the consumers' privacy concerns and their behavior in an online environment. The consumers did not adopt consumer complaining behavior with regard to privacy, did not flame, and did not complain or abstain from participating in online activities. As privacy concerns increased, they were more likely to

provide incomplete information to the web sites and less likely to register to the web sites requesting personal information.

Many consumers are troubled by the extent to which their information is collected and used; and they feel that they lost control over their own information (Muris, 2001). Muris (2001) acknowledged that despite the benefits of information sharing, concerns about privacy are real and legitimate. According to Dhillon and Moores (2001), consumers are concerned that they have no control over the personal information collected over the Internet; and companies can easily sell their personal information to a third party.

Chen and Rea (2004) identified two privacy concerns related to collection of personal information in the context of e-business: unauthorized use of personal data and giving out personal information. They found that due to privacy concerns, male users were more likely to falsify their personal information than female users; and two racial groups (African American and Caucasians) were less likely to falsify their personal information than other racial group (Asians and Hispanics). They also found that, passive control was positively related to the concern of unauthorized use of personal information and identity modification was negatively correlated with concerns of giving out personal information.

Consumers are concerned for credit card fraud and risk associated with loss of their personal information over the Internet (Nwosu, 2004). Nwosu (2004) found that consumers were concerned that they had no control of their personal information collected over the Internet and they were not aware of the use of their personal information.

Privacy policies related to control and awareness of personal information can influence customers' perceptions of fairness and trustworthiness of an online firm (Mollick, 2005). Mollick (2005) investigated effects of online vendors' policies regarding management of personal information about customers and customers' perception of fairness and trustworthiness of online firms. The results showed that the three privacy policy variables (informed consent, limiting data sharing within organizational boundary, and limiting unauthorized secondary use of data) could influence customers' perceptions of fairness and trustworthiness of an online firm.

Culnan and Armstrong (1999) found that organizations could address consumers' privacy concerns by observing procedural fairness of protecting individual privacy; and companies could gain business advantage through customer retention by observing procedural fairness. The consumers would be willing to disclose personal information when their concerns about privacy were addressed by fair procedures. Fair procedures include providing consumers with voice and control over disclosure and subsequent use of personal information.

Castaneda and Montoro (2007) found that consumers' privacy concerns related to disclosure of personal data had the strongest and the most negative effect on the user's behavior on the Internet. They also found that control over the collected information had a weak positive impact on the disclosure of personal information. Dinev, Xu, and Smith (2009) reported that perceived control of personal information was the key factor that influenced users' interaction with the Web 2.0 related sites.

Antecedents to Information Privacy Concerns

This study investigated the relationship between age, gender, and computer self efficacy, and information privacy concerns. Therefore, literature review on antecedents to information privacy concerns were limited to age, gender, and computer self-efficacy.

Age and gender have great impact on information privacy concerns (Sheehan, 1999; Zukowski & Brown, 2007). Sheehan (1999) investigated the gender differences in privacy concerns on information gathering practices by marketers using the Internet. The results showed that women were more concerned on their privacy than men; and men were more likely to adopt behaviors to protect their privacy than women.

Zukowski and Brown (2007) found that age was positively associated with the Internet Users' Information Privacy Concerns (IUIPC). As the ages of the Internet users increase, their privacy concerns also increase. Their study did not find any relationship between gender and IUIPC.

White, Shah, Cook, and Mendez (2008) examined the relationship between computer self-efficacy and four dimensions of information privacy (collection, errors, unauthorized secondary use, and improper access) posited by Smith et al. (1996). They found that there was a significant relationship between computer self-efficacy and two dimensions of privacy concerns: unauthorized secondary use of personal data and the collection of personal data; and there was no relationship between computer self-efficacy and two other information privacy concerns: errors in personal data collection and improper access of personal data. They used two measuring instruments: *Concern for Information Privacy* (CFIP) developed by Smith et al. (1996) and *Computer Self-Efficacy scale* (CSES) developed by Murphy et al. (1989). This study extended the work of White

et al. (2008) by validating their results with a broader population (different age groups and genders) and with updated scales to reflect current technology.

The literature reveals that consumers are concerned about their privacy related to collection, awareness, and control of their personal information by the direct marketers and E-commerce sites, and age, gender, and computer self-efficacy may influence an individual's privacy concerns. A summary of research studies related to information privacy concerns is shown in Appendix A.

Privacy Concerns Measuring Instruments

Given the increased concern about privacy, many Information Science researchers worked on the development and validation of scales to measure information privacy concerns related to both organization's privacy practice and the Internet users' privacy concerns. In this section, the most commonly adopted information privacy measuring instruments are discussed in chronological order.

Smith, Milberg, and Burke (1996) developed and validated a 15-item instrument with four sub-scales to measure an individual's concerns for information privacy (CFIP) regarding organizational privacy practice. The four sub-scales or dimensions (factors) of concerns for information privacy are: *collection, errors, secondary use, and unauthorized access.* The instrument was empirically validated with 186 undergraduate students, 147 graduate students, and 354 members of Information Systems and Audit Association. The Confirmatory Factor Analysis supported the validity and reliability of the instrument across these populations (Non-centralized Normed Fit Index (NCNFI) >0.9; Root Mean-squared Residual (RMR) > 0.06; Composite Reliability (CR) >0.8). The CFIP instrument

has been successfully applied within the context of offline direct marketing, but it does not measure the Internet users' privacy concerns.

Malhotra, Kim, and Agarwal (2004) developed a theoretical framework of multi-dimensional notion of Internet Users' Information Privacy Concerns (IUIPC). Their measuring instrument recognizes that there are multiple aspects of informational privacy concerns for Internet users. They introduced a 10-item scale with three dimensions of Internet users' privacy concerns: *collection, control, and awareness*. They empirically validated the 10-item IUIPC scale with 742 household respondents. The results of the Confirmatory Factor Analysis showed high value of Comparative fit index (CFI=0.94), goodness-of-fit index (GFI=0.87) and low root mean square error of approximation (RMSEA=0.051). Cronbach's alpha (CR) was found to be > 0.70 and average variance extracted (AVE) was found to be > 0.50. They suggest that IUIPC is likely to exceed CFIP as a predictor of consumer reactions to online privacy threat and IUIPC scale can be used as an updated CFIP scale to measure consumers' privacy concerns related to both organizations' management of personal information and Internet usage.

Dinev and Hart (2004) developed a 26-item scale with four dimensions (finding, abuse, vulnerability, and control) to measure Internet users' privacy concerns and two antecedents (perceived vulnerability and perceived ability) to control information. The measuring instrument was empirically validated with 369 individuals, which included the undergraduate and graduate students of a large university, the employees of four local public schools, one banking institution, three small retail and service businesses, and direct mailing services. The results showed high factor loadings (> 0.6) and high Cronbach's alpha for all four dimensions: finding (0.94), abuse (0.9), vulnerability (0.92),

and control (0.78). The results also showed that the perceived ability to control information may not be a major factor of privacy concerns when Internet transactions were involved.

Dinev and Hart (2006a) examined the relationship between information privacy concerns and e-service use; and developed a 22-item scale that categorized in five levels of information exchange: 1) surfing, 2) communicating anonymously, 3) registering unidentifiably, 4) shopping and banking, and 5) desperately seeking answers. Two dimensions of Internet privacy concerns (Privacy Concerns related to Information Finding (PCIF) and Privacy Concerns related to Information Abuse (PCIA)) were analyzed with respect to each level of information exchange. The relationships were examined using Exploratory Factor Analysis (EFA), Confirmatory Factor Analysis (CFA), and Structural Equations Modeling (SEM). The instrument was empirically validated with 369 respondents from diverse groups: the employees of private companies from different sectors, the teachers from middle and high schools, the undergraduate and graduate students. The reliability was evaluated by estimating the internal consistency through Cronbach's alpha value. Cronbach's alpha ranged from 0.77 to 0.89, which provided support for the instrument. The results showed that there were significant relationships between each of the privacy concerns (PCIF and PCIA) and Levels 2, 3, 4, and 5. The relationship between either of the privacy concerns and Level 1, which involved browsing without supplying personal information, was not significant. The results also suggested that, when using the web sites that required higher levels of information exchange, user's privacy concerns increased.

Dinev and Hart (2006b) attempted to better understand the predictors of a user's disclosure of personal information during online transaction. The research developed an 18-item scale to measure relationship between the antecedents to information privacy (Perceived Internet privacy risk, Internet privacy concerns, Internet trust, and Personal Internet interest) and the behavioral intention (willingness to disclose personal information) during online transactions. The scale was validated empirically with 369 undergraduate and graduate students of a large university in the Southeastern U.S.A. The Cronbach's alpha was greater than 0.87.

Buchanan, Pain, Joinson, and Reips (2007) developed a 28-item scale with three sub-scales to measure privacy behavior and privacy attitude of Internet users. The three sub-scales are*: privacy concerns* (privacy attitude), *general caution* (privacy behavior), and *technical protection* (privacy behavior). They conducted three studies: In study one, 515 people completed an 82-item questionnaire from which 16 privacy attitude items (privacy concerns) and 12 privacy behavior items (including both General Caution and Technical Protection) in three sub-scales were derived. The study two examined scale validity by comparing groups with different privacy concerns (technical & non technical students). The results showed that technical students reported more general caution and a higher use of technical protection than non-technical students and did not differ in privacy concerns. In study three, correlations between the scores of current scales and the measuring scale developed by Malhotra et al. (2004) were examined. The results showed a positive correlation among all scales with privacy concerns.

Castaneda and Montoro (2007) developed an 8-item scale with two dimensions to measure concern for privacy on the Internet. The dimensions are: *collection* (concern for

control over collection of personal information) and *use* (use of personal information on the electronic market). The scale was empirically validated with 440 students. The values of the Cronbach's alpha coefficient were satisfactory (0.888 for "use" and 0.802 for "collection").

Pirim, James, Boswell, Reithel, and Barkhi (2008) developed an 18-item instrument to determine an individual's need for security and privacy; and it further investigated the relationship between these two constructs. The instrument consists of a 9-item scale for security and a 9-item scale for privacy. The instrument was empirically validated using 429 students from engineering, business, and liberal arts departments. Both web-based and paper-based survey methods were used to collect data. Item loading was validated using Confirmatory Factor Analysis. Instrument's reliability was measured by calculating Cronbach's alpha value. Cronbach's alpha value for security and privacy scales were 0.9 and 0.85 respectively. A regression was run to investigate the relationship between perceived need for privacy and perceived need for security. The results showed that the instrument was reliable; and a significant relationship existed between privacy and security. Table 1 presents a summary of research studies related to privacy measuring instruments.

Table 1. Summary of Privacy Concern Measuring Instruments

Study	**Method**	**Sample**	**Measures**
Smith et al., 1966	Survey	333 students 354 auditors	A 15-item with four sub-scales: collection, errors, secondary use, and unauthorized access. Strength: 1-7.
Malhotra et al., 2004	Survey	742	A 10-item with three dimensions:

Table 1. Summary of Privacy Concern Measuring Instruments (continued)

Study	Method	Sample	Measures
		households	collection, control, and awareness. Strength: 1-7.
Dinev & Hart, 2004	Survey	369 students & professionals	A 26-item scale with four dimensions: finding, abuse, vulnerability and control. Strength: 1-5.
Dinev & Hart, 2006a	Survey	369 professionals	A 22-item scale to measure five levels of information exchange on the Internet: surfing, communicating anonymously, registering unidentifiably, shopping and banking, and desperately seeking answers. Strength: 1-5.
Dinev & Hart, 2006b	Survey	369 professionals	An 18-item scale with five sub-scales: willingness to provide personal information, perceived Internet privacy risk, Internet privacy concerns, Internet trust, and personal Internet interest. Strength: 1-5.
Castaneda et al., 2007	Survey	440 students	An 8-item scale with two dimensions: collection and use. Strength: 1-5
Buchanan et al., 2007	Survey	515 students	A 28-items with three sub-scales: privacy concerns (privacy attitude), general caution (privacy behavior), and technical protection (privacy behavior). Strength: 1-5.
Prim et al., 2008	Survey	429 students	18-item scale with 2 dimensions: security and privacy. Strength: 1-5.

Computer Self-Efficacy

Computer Self-Efficacy (CSE) is based on Bandura's broader construct of self-efficacy and its role in Social Learning Theory (SLT) (Bandura, 1986; Bandura, 1977). Self-efficacy is an individual's belief to perform certain tasks; and it is a form of self-evaluation that influences decisions about what actions to undertake when faced with obstacles (Bandura & Wood, 1989). Self-efficacy is not a measure of skill; rather, it shows what individuals believe they can do with the skills they possess. Bandura (1986) defined self-efficacy as:

> "People's judgments of their capabilities to organize and execute courses of actions required to attaining designated types of performances. It is concerned not with skills one has but with judgments of what one can do with whatever skills one possesses (p. 391)."

Computer self-efficacy represents an individual's perception of his or her ability to use computers to perform a task. Marakas, Yi, and Johnson (1998) defined computer self-efficacy as, "an individual's perception of efficacy in performing specific computer-related tasks within the domain of general computing" (p. 127). Deng, Doll, and Truong (2004) defined computer self-efficacy as, "a judgment of one's capability to use a computer in the accomplishment of a task" (p. 395). Compeau and Higgins (1995) defined computer self-efficacy as one's ability to apply his or her computer skills to a wider range of tasks.

Information Science (IS) researchers have focused on understanding the relationship between computer self-efficacy and various decision making tasks. The review of literature of computer self-efficacy study is discussed in the following two

categories: 1) relationship between computer self-efficacy and computer-supported tasks and 2) antecedents to computer self-efficacy.

Relationship between Computer Self-Efficacy and Computer-Supported Tasks

Information science researchers have focused on Bandura's (1986) Social Learning Theory (SLT) and conducted empirical studies to understand the role of computer self-efficacy and its relationship with performance of various computer-supported tasks. Computer self-efficacy (CSE) was found to be a significant predictor of performance of computer supported tasks and adoption of new technology (Hill, Smith, & Mann, 1987; Zhang & Espinoza, 1998; Urreta, 2008).

According to Hill, Smith, and Mann (1987), computer self-efficacy is an important factor in determining an individual's decision to use computers and in adopting technological advanced products. Ball (2008) found that computer self-efficacy (CSE) was the most significant contributing factor in predicting behavioral intention (BI) as it related to technology acceptance and usage. Compeau and Higgins (1995) assessed an individual's confidence in her abilities to use computer or unfamiliar software package to perform tasks. They found that training and successful interactions with computers can enhance self-efficacy

Computer self-efficacy is a significant predictor of learning and teaching using computers (Tam, 1996; Crossler & Belanger, 2006; Robinson, 2008; Huai, 2008; Ferdousi, 2009). Tam (1996) investigated the relationships between computer self-efficacy and computer skills learning for people with disability. Thirty one trainees from Hong Kong Physical Handicapped and Able-Bodied association participated in a 15-week software training program in generic Chinese computer skills. The results showed

that computer self-efficacy was a significant predictor of computer skills learning for people with physical disabilities.

Crossler and Belanger (2006) found that computer self-efficacy had a significant effect on a person's use of security tool; and instruction was not effective at increasing computer self-efficacy and use of security tool. Robinson (2008) found that computer self-efficacy was a significant predictor of intention to take additional online courses.

Ferdousi (2009) investigated the influence of computer self-efficacy (CSE) in predicting instructors' intention to use e-learning system in two years college. The results showed that CSE was a key predictor of instructors' intention to use e-learning system in two years college. Huai (2008) found that computer self-efficacy had a strong positive effect on perceived ease of use and intention of use of overhead projectors for class room teaching.

Marakas, Yi, and Johnson (1998) conceptualized the multi-dimensional nature of computer self-efficacy (CSE) construct. They theorized that CSE existed at both the general computing behavior level and at the specific computer task or application level. They analyzed existing CSE literature for various factors and issues that could have significant influence on levels of CSE and grouped them as follows: initial or prior performance characteristics, and attribution of cause; tasks characteristics and situational support; perceived effort and persistence; vicarious experience, verbal persuasion, and feedback; computer anxiety, emotional arousal, and emotion-focused coping; assigned/self-set goals, anchors, and goal commitment; gender; age; time; direction following behavior; professional orientation; issues of CSE measurement; and issues of CSE manipulation. They found that all these factors had significant relationship with

CSE. They also found that CSE measures could be subject to level effect, variability, locus, and controllability.

Computer self-efficacy (CSE) significantly predicts perceived usefulness; and perceived usefulness is a significant predictor of customers' attitudes and intentions to use Internet banking system (Ndubisi, 2006; Reid, 2008). Ndubisi (2006) examined the influence of computer self-efficacy (CSE) on the perceived usefulness, perceived ease of use, and perceived reliability of Internet banking in Malaysia. The results showed that CSE had a significant effect in the relationship between perceived usefulness, perceived ease of use, and intention to adopting Internet banking; and CSE had no effect on the relationship between perceived reliability and intention to adopting Internet banking. Reid (2008) investigated the integration of trust and computer self-efficacy (CSE) into technology acceptance model and their overall impact on customers' intentions to use banking information system in Jamaica. The results showed that CSE did not significantly predict customers' trust and perceived ease of use of banking system, but it significantly predicted perceived usefulness; and perceived usefulness was a significant predictor of customers' attitudes and intentions to use banking system.

Antecedents to Computer Self-Efficacy

Many factors can influence computer self-efficacy and can change over time (Marakas et al., 1998). Sheng and Pearson (2003) investigated the relationships between organizations' culture (teamwork, climate and morale, supervision, information flow, involvement, and meeting) and employees' computer self-efficacy. The results showed that teamwork and information flow of an organization had a significant contribution to employees' computer self-efficacy. Involvement and supervision were found to have a

negative relationship with an employees' computer self-efficacy. The meeting, climate and morale did not significantly contribute to employees' computer self-efficacy.

There is a reciprocal relationship between computer self-efficacy (CSE) and computer anxiety (Thatcher & Perrewe, 2002; Fagan, Neil, & Wooldridge, 2004). Computer anxiety refers to fear such as loss of important data or other possible mistakes regarding use of computers. Thatcher and Perrewe (2002) found that high levels of CSE caused low level of computer anxiety and low levels of CSE caused in high levels of computer anxiety. Fagan, Neil, and Wooldridge (2004) reported that experience, usage and support of computer technology were positively related to computer self-efficacy and anxiety was negatively related to computer self-efficacy; and CSE could potentially reduce computer anxiety, thereby, increasing computer usage.

There is a negative relationship between age and CSE (Reed, Doty, & May, 2005). Reed et al. (2005) found that the older people had less confidence in using computer technology than the younger people. They also found that the differences in cognitive processes, memory, learning style, and less exposure to and experience with computer technology might have inhibited older workers' abilities to use computer technology. A summary of research studies on computer self-efficacy is presented in Appendix B in chronological order.

Computer Self-Efficacy Measuring Instruments

Many researchers have used varieties of scales to measure computer self-efficacy. The most often adopted computer self-efficacy measuring instruments are discussed in chronological order.

Murphy et al. (1989) developed a 32-item computer self-efficacy scale (CSES) to measure perceptions of individuals' capabilities regarding computer-related knowledge and skills at three levels of difficulties: 1) beginning level computer skills, 2) moderate level computer skills, and 3) advanced level computer skills. The measuring scale was validated empirically with 414 students and nurses, using a 5-point Likert scale (from 1-little confidence to 5- lot of confidence) to rate their confidence levels. Through Confirmatory Factor Analysis, internal consistency and reliability coefficients (Cronbach's alphas) for three levels of confidence (beginning level, moderate level, and advanced level) were found to be of 0.97, 0.96, and 0.92 respectively.

Compeau and Higgins (1995) developed a 10-item measure of general computer self-efficacy and empirically tested the measuring scales with managers and other professionals such as insurance adjusters, financial analysts, researchers, consultants, and accountants. The scale demonstrated high internal consistency (Cronbach's alpha > 0.8). This measure has been used in varieties of contexts, and has shown good psychometric properties. The measuring scale focused on a general level of computer self-efficacy and does not align with current applications like databases, web based applications, or spreadsheets.

Kuo and Hsu (2001) developed a 12-item scale to measure ethical computer self-efficacy (ECSE). The scale was empirically validated with 186 college students. ECSE scale used three subscales: use & keep, distribution, and persuasion. The measurement of ECSE is an aggregate of these three dimensions.

Liang (2005) developed a 29-item four-dimensional scale of computer self-efficacy for use in complex technological contexts. The four dimensions are: preparatory

efficacy (7 items), performance efficacy (7 items), resources efficacy (8 items), and generative efficacy (7 items). The scale was developed from a cross-sectional survey of Enterprise Resource Planning (ERP) system users and subject matter experts; and measurement items were refined using a card sorting methodology with a sample of 10 judges. The measuring scale was tested for validity and reliability with a sample of 89 part-time MBA students of a large Northeastern University. Principal component factor analysis was done to check factor loading in each dimension. The internal consistency and reliability coefficients (Cronbach's alpha) for four dimensions (preparatory efficacy, performance efficacy, resources efficacy, and generative efficacy) were 0.95, 0.92, 0.94, and 0.92 respectively. This measuring scale does not measure today's applications like databases; web based applications, and spreadsheets.

Marakas, Johnson, and Clay (2007) studied the validity of computer self-efficacy scales over time. They compared all available measures of computer self-efficacy for their validity and stability over time and found that measuring scales may not be valid over time; and the measuring scales must evolve to reflect changes in computer technology at the current state. They proposed a 53-item scale with six sub-scales, for measuring computer self-efficacy (CSE), which reflects the current state of computer technology. The six sub-scales are: *general* computer self-efficacy, *windows* computer self-efficacy, *spreadsheet* computer self-efficacy, *word processing* computer self-efficacy, *Internet* computer self-efficacy, and *database* computer self-efficacy. The measuring construct was empirically validated with 476 students from three universities of the U.S.A. The CSE measure has two characteristics: they adhere to the base theory of the proposed framework of computer self-efficacy, and they are in keeping with the

current state of evolution within computing domain. Table 2 presents a summary of research studies related to computer self-efficacy measures.

Table 2. Summary of Computer Self-Efficacy Measures

Study	**Method**	**Sample**	**Measures**
Murphy et al., 1989	Survey	414 students	GCSE content, 32-Item, strength: 1-5
Compeau et al., 1995	Survey	1020 knowledge workers	GCSE content 10-item, magnitude: Y/N strength: 1-10.
Kuo & Hsu, 2001	Survey	186 college students	ECSE content, 12-item with three subscales: use & keep, distribution, and persuasion. Strength: 1-7.
Liang, 2005	Survey	89 students	29-item with four dimensions: performance, preparatory, resource, generative, strength: 1-10.
Marakas et al., 2007	Survey	476 students	53-items with six sub-scales: general CSE, windows CSE, spreadsheet CSE, word processing CSE, Internet CSE, and database CSE, strength: 1-10

Summary of What is Known and Unknown About the Topic

A review of privacy concern and computer self-efficacy literature was conducted to discover what is currently known and unknown about information privacy concerns and computer self-efficacy.

Consumers' privacy concerns are well founded (Pollach, 2006); and the capability of Information Technology to collect personal information has given rise to privacy concerns (Mason, 1986). Consumers are concerned about the practice of collection and control of personal information by both direct marketers (Smith et al., 1996; Phelps et al., 2000; Stuart & Segars, 2002; Dolnicar & Jordaan, 2007) and by Internet and E-commerce sites (Miyazaki & Fernandez, 2001; Chen & Rea, 2004; Chellappa & Sin, 2004; Castaneda & Montoro, 2007). Both Smith et al. (1996) and Stuart and Segars (2002) found that information privacy concerns were multi-dimensional (collection, errors, secondary use, and unauthorized access) and consumers were concerned about all dimensions of information privacy concerns. If consumers' privacy concerns are not understood and mitigated, they can have negative consequences on E-commerce growth and Internet purchases (Malhotra et al., 2004; Metzger, 2004; Phelps et al., 2000; Anton et al., 2004).

Several empirical studies (Zukovski & Brown, 2007; Sheehan, 1999) indicated that age and gender had significant effect on information privacy concerns. Sheehan (1999) found that women were more concerned about information privacy than men. Zukowski and Brown (2007) found that as the age of an Internet user increased, so did her level of privacy concerns; and did not find any relationship between genders and information privacy concerns.

Computer self-efficacy (CSE) was found to be an important factor in determining an individual's decision to use computer and to adopt technological advanced products (Hill et al., 1987; Zhang & Espinoza, 1998). An individual with higher CSE was found to have a higher outcome expectation (Compeau & Higgins, 1995a); and CSE was also found to be a significant predictor of performance of computer supported tasks and adoption of new technology (Huai, 2008; Crossler & Belanger, 2006; Ndubisi, 2006; Urreta, 2008); and learning and teaching using computers (Tam, 1996; Robinson, 2008; Ferdousi, 2009).

Little is known about how computer self-efficacy can affect an individual's information privacy concerns with respect to collection, control, and awareness of personal information collected by marketers and E-commerce sites. White et al. (2008) examined relationship between computer self-efficacy and information privacy concerns in the context of organization's practice of managing personal information; and they found that the individual with higher computer self-efficacy was less concerned with the collection of personal data and was more concerned with unauthorized use of personal data. Their study focused on the components of privacy concerns in the context of offline direct marketing (collection, errors, secondary use, and unauthorized access) and did not study component of privacy concerns in the context of Internet usage (awareness). They used students for their study and the results from their study cannot be generalized for broader population, and therefore, additional research with a broader population (different age groups and genders) to understand the relationship between computer self-efficacy and information privacy concerns have been recommended by the researchers (White et al., 2008). There is no known scholarly work to understand the differences, if

any, that may exist between different age groups and different genders' information privacy concerns, and their relationships with computer self-efficacy. This study investigated the relationship between computer self-efficacy and three components of information privacy concerns (collection, control, and awareness) posited by Malhotra et al. (2004). The study also investigated the differences among three age groups (18-25, 26-50, and 50+) and genders with respect to their relationship between computer self-efficacy and information privacy concerns.

Contribution of this Study

This study validated and extended work of White et al. (2008) and added new knowledge to information privacy concerns and computer self-efficacy research. The research results reviewed in the literature review demonstrated that information privacy concerns were complex and privacy concerns were well founded among Internet users; and computer self-efficacy was a significant predictor of behavioral intention to perform computer-supported tasks. This research provided an understanding of the relationship between computer self-efficacy and information privacy concerns. The study also examined the differences among different age groups', and between genders' regarding information privacy concerns and their relationships with computer self-efficacy. For researchers, this study addressed the relationship between information privacy concern and computer self-efficacy.

Chapter 3

Methodology

Research Methods Employed

This study was descriptive and explorative; and used a survey methodology to investigate the relationship between an individual's computer self-efficacy and his/her information privacy concerns. The study used a paper-based survey instrument and collected data by using the mall-intercept approach in which individuals were asked to fill out the survey. The participants were chosen from various places like indoor shopping areas, government buildings, coffee shops, market areas, and social gatherings, places of worships, and college campuses.

The survey instrument was developed based on validated instruments; and using empirical data, five null hypotheses were analyzed to seek answers to the research questions. This chapter is organized as follows: specific procedures employed, formats for presenting results, and resources used for this study.

Specific Procedures Employed

Survey Development

A survey for this dissertation was designed to empirically assess computer self-efficacy and information privacy concerns. Leidner and Jarvenpaa (1995) suggested that researchers should use previously validated instruments wherever possible. Consequently

the survey instrument for this study was developed by combining two existing instruments: the Computer Self-Efficacy (CSES) scale (Marakas et al., 2007) and the Internet Users' Information Privacy Concerns (IUIPC) scale (Malhotra et al., 2004). Both the instruments were empirically validated for their convergent validity and reliability. The survey instrument also contained demographics to collect certain demographic data such as age, gender, and professional status. The survey instrument is shown in Appendix C.

Demographics

This study collected the following information from the participants: *gender, age, and professional status* (student, professional, retiree, others). According to Sekaran (2003), it is advisable to collect certain demographic data such as age, gender, and professional status; such data will help to describe the sample statistics in the report.

Computer Self-Efficacy Measure

Computer self-efficacy was measured by using a 53-item CSES scale with 10-point Likert scale developed by Marakas et al. (2007). This CSES scale included items from previous scales (Compeau & Higgins, 1995; Martocchio, 1992; Martocchio & Webster, 1992; Johnson & Marakas, 2000), it reflected the base computer self-efficacy theory and it included new items to reflect current shift of the technology. The CSES scale was empirically validated by the authors. It has six dimensions: *General computer self-efficacy* (7 items- questions: CSEG1-CSEG7), *Windows computer self-efficacy* (10 items- questions: CSEW8-CSEW17), *Spreadsheet computer self-efficacy* (9 items – questions: CSES18-CSES26), *Word-processing computer self-efficacy* (7 items- questions: CSEW27-CSEW33), *Internet computer self-efficacy* (10 items- questions:

CSEI34-CSEI43), and *Database computer self-efficacy* (10 items- questions: CSED44-CSED53).

Information Privacy Concerns Measure

Information privacy concerns were measured by a 10-item IUIPC scale with 7-point Likert scale developed by Malhotra et al. (2004). It measured information privacy concerns of management of personal information by the organizations and Internet users' privacy concerns. It has three dimensions: *control* (3 items- questions: PCON1-PCON3), *awareness* (3 items – questions: PAW4-PAW6), and *collection* (4 items- questions: PCOL7-PCOL10). The IUIPC scale was empirically validated by the authors. It is an updated CFIP scale (Smith et al, 1996) with an additional dimension (awareness) to measure Internet users' privacy concerns.

Population and Sample

The target population of this study was the residents of the state of New Jersey, U.S.A over 18 years of age. The total sample size of this study was 400 subjects in three age groups: 18-25, 26-50, and 50+. White et al. (2008) stressed the need of a study where subjects would be composed of traditional students and adult professionals. These three age groups were chosen to include traditional students (18-25), adult professionals (26-50), and mature adults (50+). Since the study compared findings among the three age groups and genders, the stratified sampling method was used to preserve representativeness of each group. According to Barlett, Kotrlik, and Higgins (2001), the minimum returned sample size for a given population of size greater than 4000 should be 119 for continuous data with alpha=0.05 and beta=0.03; and based on their recommendation, the sample size for each age and gender group was more than 119.

Data Collection

The data collection procedure was through face-to-face interaction with the participants using a mall-intercept approach in which individuals were approached to complete the survey. Personal interaction method eliminated and reduced response rate error and guaranteed required returned sample size. Face-to-face interaction also improved data quality by improving item non-response rate (Heerwegh & Loosveldt, 2008). Several researchers (Stewart & Segars, 2002; Hornsby, 2007) used similar mall-intercept technique for their research. In order to find participants in all age groups, data was collected at different times of the day (morning, noon, and evening) and on different days of the week (week days and weekends). To attract a participant, a monetary reward of $2 was offered to the participant for her time in filling up the survey questionnaire. Monetary incentive was found to be effective method to attract the respondents and to improve participation (Hornsby, 2007; Zagorsky & Rhoton, 2008).

Prior to the actual study, a pilot study was conducted to test the measuring instrument and the overall design methodology. The pilot study determined the average time to complete the survey questions and verified effectiveness of the instruments. The size of the pilot study was 36 participants, equally spread across three age groups and two genders. Robinson (2008) used 40 participants for his pilot study and Nakos (2003) used 36 participants for his study. The approval from the Institutional Review Board (IRB) of Nova Southeastern University was requested and data collection started only after receiving approvals from the IRB and the dissertation committee members.

Pre-Analysis Data Screening

According to Mertler and Vannatta (2001), pre-analysis data screening is required prior to major data analysis to ensure that the results and the conclusions are made based on valid data. As per Levy (2006) pre-analysis of data screening for an empirical study should be done to ensure accuracy of the data collected, to deal with the issue of response-set, to deal with missing data, and to deal with outliers or extreme cases.

With the mall-intercept approach, where the researcher was available to provide clarity of the survey questions, data entry errors were reduced. However, the data was reviewed prior to running data analysis to ensure the accuracy of data. The response-set is where respondents submit the same score for all items. Data collected for this study was reviewed for response-sets and was considered for elimination from the final analysis. Due to data collection method (face-to-face interaction), missing data may not be an issue for this study. However, data collected for this study was reviewed for missing data and was considered for elimination from the final analysis.

An outlier is an observation that lies outside the overall pattern of the data. Statistical Package for Social Science (SPSS), version 18 (PASW statistics 18) was used for outlier detection. Both univariate and multivariate analyses were performed to detect outliers. Univariate outliers are cases that have an unusual value (extreme high or extreme low value) for a single variable. The univariate analysis was done using standard scores (z-score), boxplot, and descriptive statistics. For a sample size larger than 80 items, an item is an outlier if its standard score is ±3.0 or beyond (McClave, Benson, & Sincich, 2005). The variables of interests were: information privacy concerns (dependent variable) and computer self-efficacy (independent variable). The additive score of computer self-efficacy (CSETOT) and information privacy concerns (PTOT) were used

for the analysis. Descriptive statistics was computed for mean (μ) and standard deviation (σ) for CSETOT and PTOT. Before making decision whether an item can be omitted or retained, the value for each variable, which was detected as an outlier, was compared to the mean and standard deviation of the variable. If the value was found to be beyond mean ± standard deviation, then only the item would be omitted. The multivariate analysis was done using Mahalanobis distance analysis on both CSETOT and PTOT. Data of extreme cases was eliminated from final analysis. According to Sun, Omachi, Kato, Aso, Kono, and Takagi (2000), Mahalanobis distance is widely used technique for distance measure and outlier detection.

Validity and Reliability

The construct and content validity of this study was achieved by basing survey items on previously validated scales. To determine inter-item reliability and internal consistency for each scale, Cronbach's alpha reliability test was performed for each of the scales (CSES & IUIPC) and their dimensions. Nunnally and Bernstein (1994) provided guidance in the interpretation of the reliability coefficient by stating that a value of .70 is sufficient for early stages of research, but that basic research should require test scores to have a reliability coefficient of .80 or higher.

Data Analysis

Data was analyzed by three age groups (18-25, 26-50, and 50+) and by genders. Statistical analyses were performed to address the two specific research questions: 1) is there a relationship between an individual's information privacy concerns and her

computer self-efficacy? and 2) is there any difference among age groups (18-25, 26-50, 50+) and different genders (male and female) with respect to their relationship between computer self-efficacy and information privacy concerns? Data analysis for this study included demographics, descriptive statistics, bivariate normality analysis, correlation analysis, hypotheses testing, and analysis of research questions. MS Excel and Statistical Package for Social Science (SPSS) for Windows version 18 were used for data preparation and data analysis.

Demographics

To provide accurate answers to the research questions, the sample used must be representative of the population (Sekaran, 2003); and must meet the minimum sample size (N=>119) (Barlett et al., 2001). Therefore, the demographic data (gender, age, professional status) were requested from the survey participants.

Descriptive Statistics

Descriptive statistics included computation of min, max, mean and standard deviation for variables of interest. The variables of interest were: total additive score of 10 items of information privacy concerns (PTOT) and total additive score of 53 items of computer self-efficacy (CSETOT).

Bivariate Normality Analysis

For bivariate normality tests for both dependent (PTOT) and independent (CSETOT) variables, graphical (histogram, Probability-Probability plot (P-P plots), and Quantitle-Quantitle plot (Q-Q plots) and a theoretical method (Shapiro-Wilk test) were used. A histogram of both dependent and independent variables showed rough normality. The straighter the line formed by the P-P plot, the more the variable's distribution

conformed to the normal distribution of data. A Q-Q plot formed a 45-degree line when the observed values were in conformity with the hypothetical distribution. The Shapiro-Wilk test for normality determined if the item values were distributed Gaussian. Scatter diagram helped us to visualize any apparent relationship between variables of interests (CSETOT, PTOT).

Correlation Analysis

The correlation analysis included computation of correlation coefficient and significance of relationship. The nonparametric correlation analysis method (Spearman rank-order) was used to determine the relationship. The value of correlation coefficients ranges from +1 to -1.The value of correlation coefficient closure to +1 showed significant positive relationship and its value closure to -1 showed significant negative relationship. If there was no relationship between the variables of interests, then the value of correlation coefficient would be near zero. Multivariate analysis of variances (MANOVA) was used to compare means of dependent (PTOT) and independent (CSETOT) variables between genders and among age groups.

Hypotheses Testing

Five null hypotheses were tested by using the Spearman rank-order test of nonparametric correlation analysis. If the observed significance level or a p-value was found to be less than 0.05, then the hypothesis would be rejected.

Analysis of Research Questions

The answer to the first research question was sought from the testing of hypothesis 1. If hypothesis 1 was rejected, then the correlation between CSE and IPC was significant. The value of correlation coefficient closure to +1 will show significant

positive relationship and its value closure to -1 will show significant negative relationship.

To seek answer to the second research question, three statistical methods were used: testing of hypotheses 2, 3, 4, and 5, the Spearman rank-order test, and the MANOVA test. By comparing the differences in correlations from hypotheses testing, differences in correlation coefficients from the Spearman rank-order tests, and differences in mean values from the MANOVA tests, correlation differences between genders and among age groups were concluded. The analyses were done in two steps: the first step included analyses for finding differences between genders with respect to their relationship between CSE and IPC, and the second step included analyses for finding differences among three age groups (18-25, 26-50, and 50+) with respect to their relationship between CSE and IPC.

To find correlation differences between genders, hypotheses 3 and 5 were evaluated; and correlation analysis using the Spearman rank-order tests were performed between IPC and CSE for each of the genders. The MANOVA tests were done to find the significance of differences of mean values of the variables (PTOT, CSETOT) between genders.

To find correlation differences among age groups, hypotheses 2 and 4 were evaluated; and the Spearman rank-order tests were performed between IPC and CSE for each of the age groups. The MANOVA tests were done to find the significance of differences of mean values of the variables (PTOT, CSETOT) among age groups.

Formats for Presenting Results

The results from the data analyses were presented in various tables and figures in chapter four. The results of the outlier analysis were presented in figures as box plots. The results of the descriptive statistics, reliability tests (Cronbach's alpha value), the correlation coefficients (ρ), and p-value for the hypotheses evaluation were presented in tables. P-P plots, Q-Q plots, and scatter diagram were presented in figures.

Resources

A personal computer with MS Word was used to write report and to develop the paper-based survey instrument. MS Excel and the Statistical Package for Social Science (SPSS) were used for data preparation, data analysis and data validation. Survey participants of the state of New Jersey, U.S.A and accesses to libraries were essential parts of this study.

Summary

This study was descriptive and explorative. A survey methodology was used to investigate the relationship between computer self-efficacy and information privacy concerns. A paper-based survey instrument, using two validated scales, was developed. The target population of this study was the residents of New Jersey, U.S.A over 18 years of age. The sample size for this study was 400 participants from different age groups and genders. The stratified sampling method was used to preserve representativeness of each of the age groups and gender. The data collection procedure was through personal interaction using the mall-intercept approach, in which an individual was approached within indoor shopping areas, government buildings, coffee shops, and social gatherings, places of worships, college campuses, and market areas to complete the survey.

Pre-analysis of data screening was done to eliminate bad data. Data analysis methods included the testing of five hypotheses, computation of descriptive statistics, demographics, and analysis of research questions. Five null hypotheses were tested by using observed significance level or p-value approach with 95% confidence level (if $p <= \alpha$ (0.05), reject null hypotheses). Descriptive statistics included computation of mean, min, max, and standard deviation for variables of interest (IPC and CSE). Correlation analysis included bivariate normality analysis and computation of correlation coefficient using Spearman rank-order test.

A personal computer with MS Word was used to write report and to develop the paper-based survey instrument. MS Excel and SPSS were used for data preparation, data analysis and data validation.

Chapter 4

Results

Pilot Study

Prior to the actual study, a pilot study was conducted to test the measuring instrument. It involved 36 participants. The participants were spread equally across each age group (12 from age 18-25, 12 from26-50, and 12 from 50+). Among the participants, 72.2% was male and 27.8% was female. The demographic data of the participants is shown in table 3.

Table 3. Demographic Data for Pilot Study (N=36)

Subjects	**Frequency**	**Percent (%)**
Female (F)	10	27.8
Male (M)	26	72.2
Age group-18-25	12	33.3
Age group-26-50	12	33.3
Age group-50+	12	33.3
Total participants	36	100

The survey was conducted through face-to-face interaction where the participants were asked to fill out the survey questions. On an average, the pilot group took 20 minutes to complete the survey. The participants were chosen randomly from New

Jersey, U.S.A. The monetary reward of $2 was offered to the participants for their time in filling out the survey questions. But it was not effective in attracting participants to fill out the survey. Only one participant accepted the monetary reward. When the purpose of the research was explained to the participants and when they were assured that no personal information would be collected through the survey, then only the participants were willing to participate. Reliability analysis was performed on both computer self-efficacy and information privacy concerns scales by computing Cronbach's alpha value for each of the scales. The computer self-efficacy scale had Cronbach's alpha value of 0.998 with 53 items and information privacy concerns scale had Cronbach's alpha value of 0.8. Table 4 presents the results of reliability tests. Both the scales had values for alpha that exceeded the criterion of 0.7 which was the minimal value suggested for internal consistency reliability (Nunnally & Bernstein, 1994).

Table 4. Reliability Coefficients for Pilot Study

Scale	Number of Items	Cronbach's Alpha Value
Computer Self-Efficacy (CSES)	53	0.998
Information Privacy Concerns (IUIPC)	10	0.800

The computer self-efficacy (CSE) was measured by adding Likert scale scores of all 53 items of CSES construct; and the additive score was saved as CSETOT. The information privacy concerns (IPC) was measured by adding Likert scale scores of all 10 items of IUIPC construct; and the additive score was saved as PTOT. For 36 participants, the mean value of CSETOT was found to be 396.39 with standard deviation of 182.531;

and the mean value of PTOT was found to be 64.06 with standard deviation of 6.118. The descriptive statistics of the pilot study is shown in tables 5.

Table 5. Descriptive Statistics for Pilot Study

	N	Minimum	Maximum	Mean	Std. Deviation
CSETOT	36	53	530	396.39	182.531
PTOT	36	47	70	64.06	6.118

The results from the pilot study showed that the questions were clear. Few respondents asked questions on some survey questions. Most of the participants understood the questions. Both the scales (CSES and IUIPC) had high internal consistency coefficients. The Cronbach's alpha values for CSES and IUIPC were found to be 0.998 and 0.800 respectively. Therefore, the survey instrument was deemed reliable to use for the study.

Actual Study

Like the pilot study, data for the actual study was obtained through face-to-face interaction with the participants using a paper based survey. The participants were selected randomly from various places of the state of New Jersey (University campus, shopping malls, coffee shops, places of worships, and various places of social gatherings). The appendices D and E show the approval letters from the Institutional Review Boards (IRB) of Nova Southeastern University and of Rider University respectively. The appendix F shows the permission letter from the Menlo Park mall. Data from 415 participants were collected within a period of two months (July 2010- August

2010). The participants were offered a monetary reward of $2 for their time to fill out the survey. The monetary reward to attract participants to fill out survey questionnaire was not found to be very effective. Only very few participants responded to monetary reward. When the purpose of the research was explained to the participants with the assurance of anonymity and guarantee of no personal information in the survey questionnaire, then the participants were more willing to participate in filling out the survey questions. From the paper survey, the data was entered manually to MS Excel and each respondent was assigned a number (1-415) for tracking purpose.

Pre-Analysis Data Screening

To ensure that the results and conclusions were made based on valid data, the pre-analysis data screening was conducted before final analysis. First, each survey item was checked manually for any missing data. Second, univariate and multivariate analyses were done to detect outliers. One survey item (item #19) was found to have missing data and that item was removed. In univariate outlier analysis, standard score for CSETOT for 7 items with tracking numbers of 179, 305, 340, 395, 397, 414, and 415 were found to have values < -3.0 and no item had standard score >3.0. The boxplot of standard score of CSETOT is shown in figure 2. The standard score for PTOT for 7 items with tracking numbers of 10, 105, 174, 186, 192, 323, and 388 were found to have values < -3.0 and no item had standard score >3.0. The boxplot of standard score of PTOT is shown in figure 3. For a sample size larger than 80 items, an item is an outlier if its standard score is ±3.0 or beyond (McClave, Benson, & Sincich, 2005). The additive score of items, that were identified as outliers for extreme low values for both PTOT and CSETOT, were

compared to mean and standard deviation of PTOT and CSETOT respectively; and they were found to have values $< \mu - \sigma$.

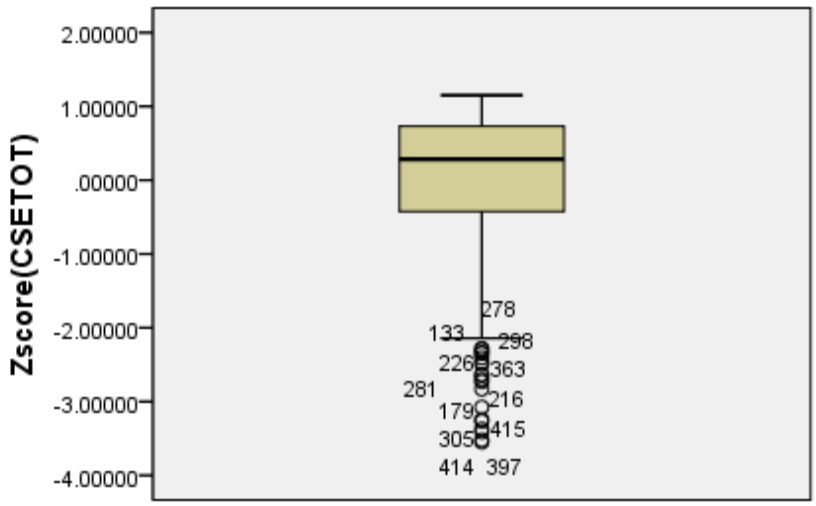

Figure 2. Boxplot for independent variable (CSETOT).

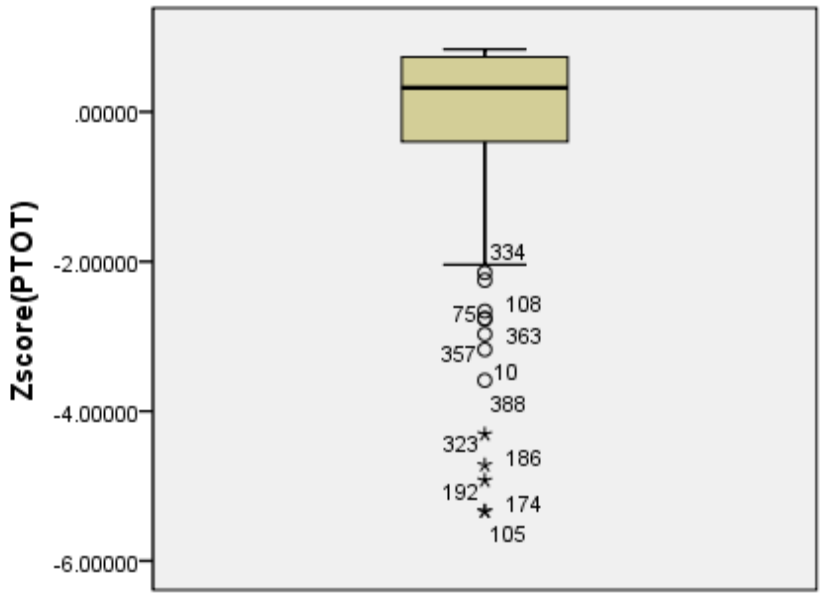

Figure 3. Boxplot for dependent variable (PTOT).

Therefore, these 14 items were omitted from final analysis. The additive Likert scale scores of items that were identified as outliers, mean and standard deviation for both CSETOT and PTOT are shown in table 6.

Table 6. Outliers - Values, Mean and Standard Deviation

Variables	**Additive score***	**Mean**	**Standard Deviation**
CSETOT	53, 56, 67, 71, 82, 84, 101	413.20	101.479
PTOT	10,10, 14, 16, 20, 27, 31	61.86	9.718

*Additive score (CSETOT- additive Likert scale scores of 53 items of CSE scale; PTOT- additive Likert scale scores of 10 items of IUIPC scale)

Multivariate analysis was done on both independent (CSETOT) and dependent variables (PTOT) using Mahalanobis distance analysis. From the multivariate analysis, no outliers were detected. Therefore, 15 items were omitted (1 with missing data and 14 outliers) and 400 survey items were used for final analysis.

Validity and Reliability

The construct and content validity of the survey instrument was achieved by basing survey items on previously validated scales. The reliability of the instrument was examined by conducting Cronbach's alpha reliability test for each of the scales (CSES & IUIPC) and their dimensions (six dimensions of CSES and three dimensions of the IUIPC scales). Both the scales and their dimensions were found to have values for alpha that exceeded 0.7 which was the minimal value suggested for internal consistency reliability (Nunnally & Bernstein, 1994). Cronbach's alpha values were found to be 0.981 and 0.879 for CSES and IUIPC scales respectively. For six dimensions of CSES scale,

Cronbach's alpha values were found to be 0.923, 0.954, 0.970, 0.950, 0.936, and 0.985 for *General* CSE, *Windows* CSE, *Spreadsheet* CSE, *Word-processing* CSE, *Internet* CSE, and *Database* CSE respectively. For three dimensions of IUIPC scale, Cronbach's alpha values were found to be 0.765, 0.710, and 0.912 for *Control*, *Awareness*, and *Collection* respectively. The results of the reliability tests are shown in table 7.

Table 7. Reliability Coefficients for Actual Study

Constructs	Dimensions	Cronbach's alpha value
Computer Self-Efficacy (CSES)	General	0.923
	Windows	0.954
	Spreadsheet	0.970
	Word-processing	0.950
	Internet	0.936
	Database	0.985
Total CSE*		**0.981**
Information Privacy Concerns (IUIPC)	Control	0.765
	Awareness	0.710
	Collection	0.912
Total IPC**		**0.879**

* Cronbach's alpha value was calculated on additive Likert scale scores of all six dimensions of CSES
** Cronbach's alpha value was calculated on additive Likert scale scores of all three dimensions of IUIPC

Data Analysis

For final analysis, 400 survey items were used. The variables of interests were: information privacy concerns (IPC), computer self-efficacy (CSE), age, and gender. An individual's information privacy concerns (IPC) was calculated by adding Likert scale

scores of all 10 items of the IUIPC scale; and the additive score for IPC was saved as PTOT. Computer self-efficacy (CSE) was measured by adding Likert scale scores of all 53 items of the CSES scale; and the additive score of CSE was saved as CSETOT. CSETOT and PTOT are ordinal data. The PTOT is the dependent variable and the CSETOT is the independent variable. Since, age and gender are nominal data, for correlation analysis, these variables were transformed to ordinal data as:

1. age => age2, recoding data as: 18-25 => 1, 26-50=> 2, and 50+ => 3
2. gender => gender2, recoding data as: M=>1 and F=>2

The age2 and gender2 were transformed ordinal variables for age and gender respectively. Data analysis included demographics, descriptive statistics, bivariate normality analysis, hypotheses testing, and analysis of research questions.

Demographics

To provide accurate answers to the research questions, the sample used must be representative of the population (Sekaran, 2003) and must meet the minimum sample size (N=>119) (Barlett et al., 2001). Therefore, the demographic data (gender, age, professional status) were requested from the survey participants. The total sample size of this study was 400 survey items. The distribution appeared to be representative of the population. Two hundred thirty-seven (59.25%) were male participants and 163 participants (40.75%) were female. The sample size for male (237) and that of female (163) exceeded the minimum sample size requirement (N=>119). With respect to age groups, 123 participants (30.75%) were from the age group of 18-25, 154 participants (38.5%) were from age group of 26-50, and 123 participants (30.75%) were from the age group of 50+. The participants were almost equally divided among age groups and the

sample size exceeded the minimum sample size requirement (N=>119). Most of the precipitants were working professionals (59%) and most of the participants in age group of 18-25 were under graduate students. Table 8 shows the demographic data of the participants.

Table 8. Demographic Data for Actual Study (N=400)

Variable	Frequency	Percentage
Gender		
Male	237	59.25
Female	163	40.75
Ages in years		
18-25	123	30.75
26-50	154	38.5
50+	123	30.75
Professional Status		
Professional	236	59.00
Graduate Students	20	5.00
Under Graduate Students	128	32.00
Retiree	12	3.00
Others	4	1.00

Descriptive Statistics

The descriptive statistics included the computation of min, max, mean, and standard deviation of variables of interest. The variables of interest were: total additive score of all 53 items of computer self-efficacy scale (CSETOT) and total additive score of all 10 items of information privacy concerns (PTOT). The maximum scores were found to be 530 and 70 for CSETOT and PTOT respectively. The mean score for

CSETOT was found to be 419.35 with standard deviation of 91.992. The mean score for PTOT was found to be 62.52 with standard deviation of 7.881. The minimum values were found to be 126 and 33 for CSETOT and PTOT respectively. The table 9 shows the descriptive statistics of the study.

Table 9. Descriptive Statistics of Variables

	N	Minimum	Maximum	Mean	Std. Deviation
CSETOT	400	126	530	419.35	91.992
PTOT	400	33	70	62.52	7.881

Bivariate Normality Analysis

The bivariate normality analysis included graphical methods (histograms, scatterplot, P-P plots, and Q-Q plots) and theoretical method (Shapiro-Wilk test). The histograms were plotted for both CSETOT and PTOT. The histogram for CSETOT is shown in figure 4 and histogram for PTOT is shown in figure 5.

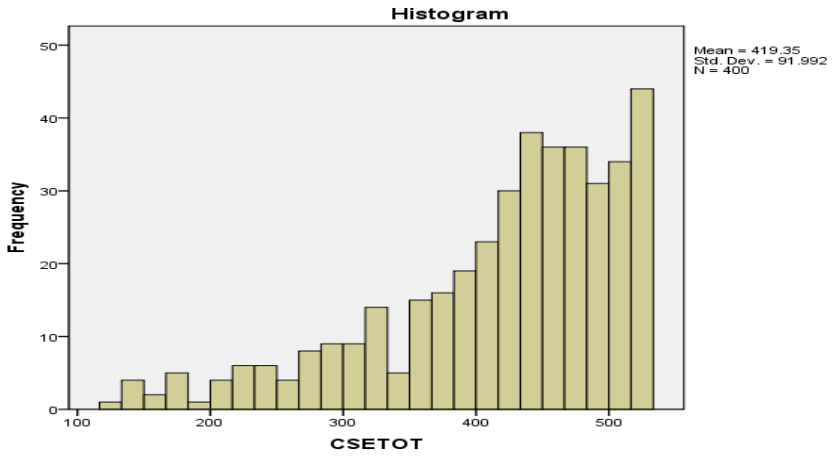

Figure 4. Histogram for CSETOT

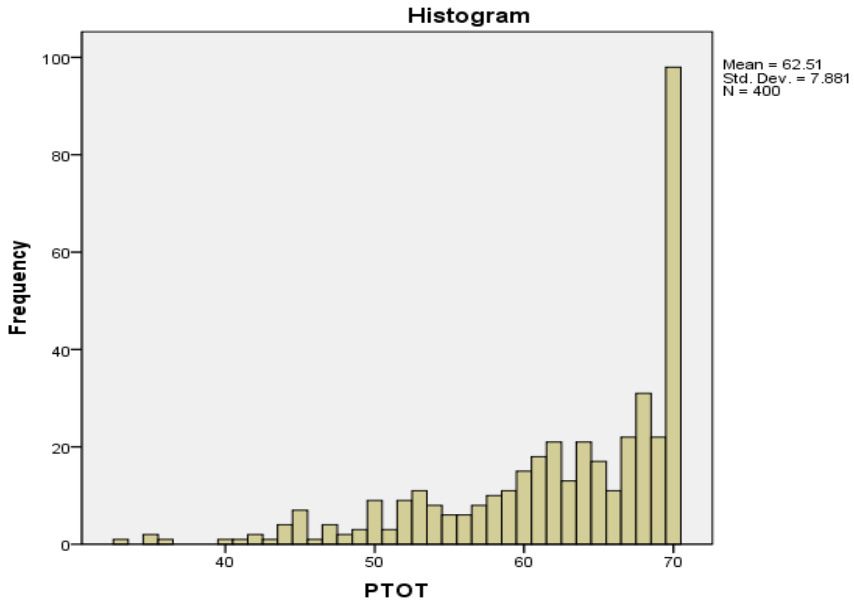

Figure 5. Histogram for PTOT

The histograms for both CSETOT (figure 4) and PTOT (figure 5) showed that data were skewed to the left. The P-P plots for PTOT is shown in figure 6, and P-P plot for CSETOT is shown in figure 7.

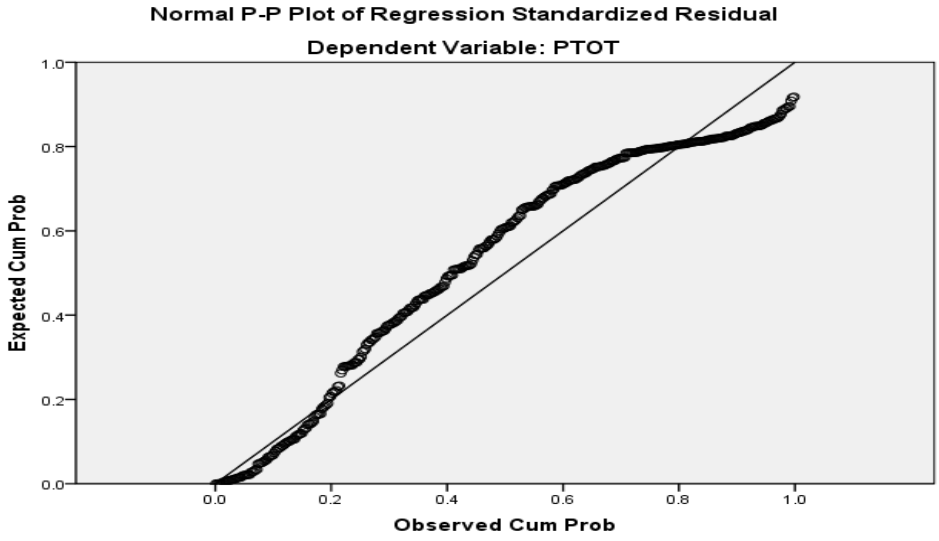

Figure 6. P-P plot for PTOT

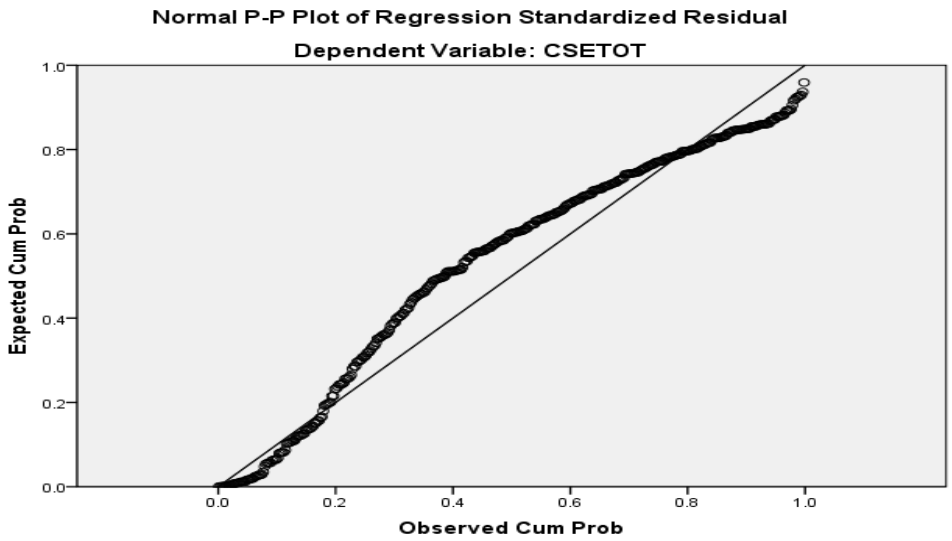

Figure 7. P-P plot for CSETOT

The P-P plots for both PTOT (figure 6) and CSETOT (figure 7) depicted the deviation of data points from the straight line. The Q-Q plots for CSETOT and PTOT are shown in figures 8 and 9 respectively.

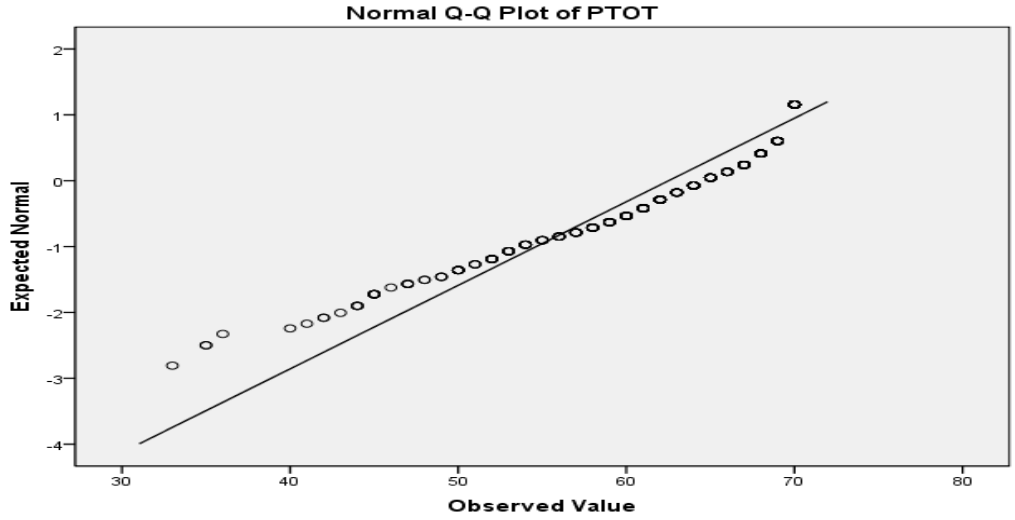

Figure 8. Q-Q plot for PTOT

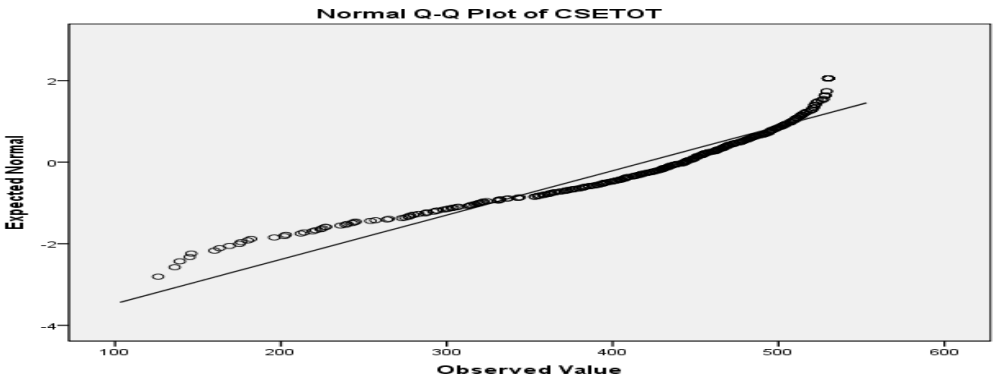

Figure 9. Q-Q plot for CSETOT

The Q-Q plots for both PTOT (figure 8) and CSETOT (figure 9) depicted the deviation of data points from the straight line. To evaluate the relationship between information privacy concerns and computer self-efficacy, a scatter diagram was plotted with PTOT as dependent variable and CSETOT as independent variable. Figure 10 shows scatter diagram for PTOT and CSETOT. The scatter diagram does not show a strong linear relationship between PTOT and CSETOT.

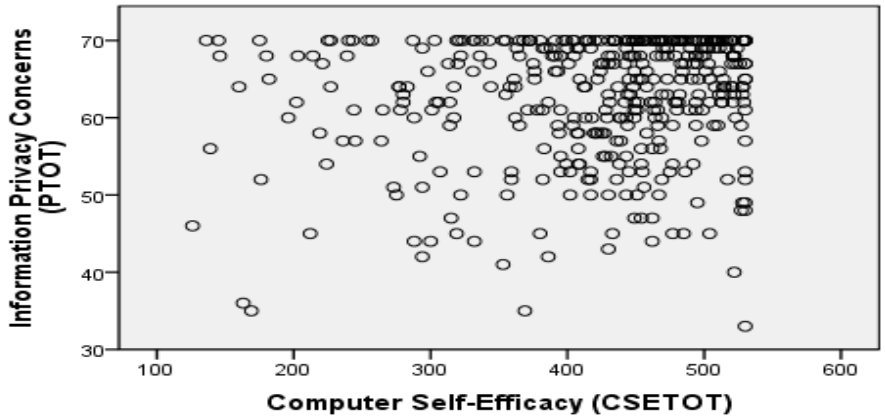

Figure 10. Scatterplot between PTOT and CSETOT.

The histograms, P-P plots, Q-Q plots, and scatterplot showed that data was not normally distributed. The Shapiro-Wilk tests were also performed to test normality of

data for both the variables (CSETOT and PTOT). The Shapiro-Wilk test also rejected the normality of data (p-value= 0.000) at 0.01 level. The result of the test is shown in table 10.

Table 10. Test of Normality using the Shapiro-Wilk test

	Shapiro-Wilk		
	Statistic	**df**	**Sig.**
PTOT	.862	400	.000*
CSETOT	.902	400	.000*

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

Hypotheses Testing and Findings

Since the results from the bivariate analysis showed that the dataset was not normally distributed, the Pearson correlation analysis was not used; instead nonparametric the Spearman rank-order correlation test were used to identify relationship between the hypothesized independent variables and dependent variable.

Hypothesis 1

H_{01}: There is not a significant relationship between an individual's concern for information privacy and her computer self-efficacy.

The Spearman rank-order test was performed between PTOT and CSETOT where, PTOT was an additive score of IPC construct and CSETOT was an additive score of CSE construct. The correlation coefficient for Spearman rank-order test was found to be 0.128 with significant value (p-value) of 0.010. The correlation was positive, but the magnitude was low. The correlation was significant at 0.05 level. When a person's computer self-efficacy increases, her information privacy concerns also increase. Based

on this test, hypothesis 1 is rejected. The result of Spearman rank-order test between computer self-efficacy (CSETOT) and information privacy concerns (PTOT) is shown in table 11.

Table 11. Results of Spearman rank-order test between CSETOT and PTOT

			CSETOT	**PTOT**
Spearman's rho	CSETOT	Correlation Coefficient	1.000	.128*
		Sig. (2-tailed)	.	.010
		N	400	400
	PTOT	Correlation Coefficient	.128*	1.000
		Sig. (2-tailed)	.010	.
		N	400	400

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

H_{02}: There is not a significant relationship between information privacy concerns and age groups.

Since the Spearman rank-order test works on ordinal value only, data of age groups were transformed into an ordinal data as 18-25 => 1, 26-50 => 2, and 50+ => 3. The Spearman rank-order test was performed between PTOT and age2 where, PTOT was an additive score of IPC construct and age2 was the transformed ordinal variable for age. PTOT was the dependent variable and age2 was the independent variable. The correlation coefficient between PTOT and age2 was found to be 0.342 with significant value (p-value) of 0.000. The correlation was positive, but the magnitude was low. The p-value is 0.000; and therefore, the relationship was significant at 0.01 level. Based on this test, hypothesis 2 was rejected. There is a significant positive relationship between individual's concerns for information privacy and her age. An individual's information

privacy concerns increase with the increase of her age. The test result is shown in table 12.

Table 12**.** Results of Spearman rank-order test between PTOT and Age

			PTOT	**Age2**
Spearman's rho	PTOT	Correlation Coefficient	1.000	.342**
		Sig. (2-tailed)	.	.000
		N	400	400
	Age2	Correlation Coefficient	.342**	1.000
		Sig. (2-tailed)	.000	.
		N	400	400

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

H_{03}: There is not a significant relationship between information privacy concerns and gender.

The Spearman rank-order test was performed between PTOT and gender2 where, PTOT was an additive score of IPC construct and gender2 was the transformed ordinal variable for gender. PTOT was the dependent variable and gender2 was the independent variable. The independent variable (gender2) was transformed from nominal variable (gender) to ordinal variable as M => 1 and F => 2. The correlation coefficient between PTOT and gender2 was found to be 0.033 with significant value (p-value) of 0.505. The correlation was positive, but the magnitude was very low. The p-value exceeds α=0.05; and therefore, the relationship was not significant at 0.05 levels. Based on this test result, hypothesis 3 is not rejected. The correlation was not statistically significant. The test result from correlation analysis is shown in table 13.

Table 13**.** Results of Spearman rank-order test between PTOT and Gender

			Gender	**PTOT**
Spearman's rho	Gender	Correlation Coefficient	1.000	.033
		Sig. (2-tailed)	.	.505
		N	400	400
	PTOT	Correlation Coefficient	.033	1.000
		Sig. (2-tailed)	.505	.
		N	400	400

H_{04}: There is not a significant relationship between computer self-efficacy and age groups.

The Spearman rank-order test was performed to compute the correlation coefficient and significance of the relationship between CSETOT and age2 where, CSETOT was an additive score of computer self-efficacy (CSES) scale and age2 was the transformed ordinal variable for age. CSETOT was the dependent variable and age2 was the independent variable. The correlation coefficient between CSETOT and age2 was found to be -0.121. The correlation was negative and the magnitude was low. The p-value was 0.015; and therefore, the correlation was significant at 0.05 level. Based on this test, hypothesis 4 was rejected. Computer self-efficacy decreases with the increase of age. The test result is shown in table 14.

Table 14. Results of Spearman rank-order test between CSETOT and Age

			Age	CSETOT
Spearman's rho	Age	Correlation Coefficient	1.000	-.121*
		Sig. (2-tailed)	.	.015
		N	400	400
	CSETOT	Correlation Coefficient	-.121*	1.000
		Sig. (2-tailed)	.015	.
		N	400	400

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

H_{05}: There is not a significant relationship between computer self-efficacy and gender.

The Spearman rank-order test was performed to compute the correlation coefficient and significance of the relationship between CSETOT and gender2 where, CSETOT was an additive score of CSE construct and gender2 was the transformed ordinal variable for gender (M=>1, F=>2). The correlation coefficient was found to be -0.170 with significant value (p-value) of 0.001.The correlation was negative, but the magnitude was low. The relationship was significant at 0.01 level. Based on this test, hypothesis 5 was rejected. The test result from correlation analysis is shown in table 15.

Table 15. Results of Spearman rank-order test between CSETOT and Gender

			CSETOT	Gender
Spearman's rho	CSETOT	Correlation Coefficient	1.000	-.170**
		Sig. (2-tailed)	.	.001
		N	400	400
	gender	Correlation Coefficient	-.170**	1.000
		Sig. (2-tailed)	.001	.
		N	400	400

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

From the results of the hypotheses testing, hypotheses 1, 2, 4, and 5 were rejected. Only hypothesis 3 was supported. Table 16 shows results of hypotheses testing.

Table 16. Hypotheses Test Results

Hypothesis	**Rejected**	**Supported**	**Spearman rank-order Correlation Coefficient (ρ)**	**Significance (p-value)**
H_{01}	YES	NO	0.128	0.010
H_{02}	YES	NO	0.342	0.000
H_{03}	NO	YES	0.033	0.505
H_{04}	YES	NO	-0.121	0.015
H_{05}	YES	NO	-0.170	0.001

Analysis of Research Questions

There are two research questions for this study. The answer of the first research question was sought from the testing of hypothesis 1 and the answer to the second question was sought by comparing correlation coefficients between genders and among age groups with respect to their relationship between information privacy concerns and computer self-efficacy.

Research Question 1**:** Is there a relationship between an individual's information privacy concerns and her computer self-efficacy?

This research question was evaluated through the testing of hypothesis 1. The result showed that there was a significant positive relationship between an individual's information privacy concerns and her computer self-efficacy. But the magnitude was low. The correlation was significant at 0.05 level. An individual's information privacy concerns increase with the increase of her computer self-efficacy.

Research Question 2: Is there any difference among different age groups (18-25, 26-50, 50+) and between genders with respect to their relationship between computer self-efficacy and information privacy concerns?

To seek an answer to this research question, three methods were used: the first method was the correlation analysis between information privacy concerns (IPC) and computer self-efficacy (CSE) for each of the age groups and genders, the second method was the MANOVA test to compare means of IPC and CSE between genders and among age groups, and the third method was evaluating results of tests of hypotheses 2, 3, 4, and 5.

The Spearman rank-order tests were performed for both gender and age groups. The Spearman correlation coefficients were found to be 0.129 and 0.153 for male and female respectively. The correlation for male was found to be significant at 0.05 level ($p=0.048$). But the correlation for female was not significant at 0.05 level ($p=0.051$). Female participants were found to have higher correlation coefficient than male participants. The Spearman rank-order test was performed on each of the age groups. The Spearman correlation coefficients were found to be 0.088, 0.228 and 0.125 for age groups of 18-25, 26-50, and 50+ respectively. The correlations for age groups of 18-25 ($p=0.330$) and 50+ ($p=0.169$) were not significant at 0.05 level. But the correlation for age group of 26-50 was significant ($p=0.005$) at 0.01 level. The magnitude of correlation coefficient for age group of 26-50 was much higher than correlation coefficients of other two age groups (18-25 and 50+). The results of the correlation tests for gender and age groups are shown below in table 17.

Table 17. Correlation coefficients for Gender and Age

Groups	Spearman rank-order coefficient	P-value
Gender- Male	0.129	**0.048***
Gender- Female	0.153	0.051
Age -18-25	0.088	0.330
Age -26-50	0.228	**0.005****
Age -50+	0.125	0.169

* correlation is significant at 0.05 level
** correlation is significant at 0.01 level

The multivariate analysis of variances (MANOVA) was performed to compare means of dependent variables (PTOT and CSETOT) for gender. The results showed that the female participants had slightly higher means of information privacy concerns, but the difference of means of information privacy concerns between male and female was not significant at 0.05 level (p=0.227). Male participants were found to have higher computer self-efficacy than female and the difference of means of computer self-efficacy between male and female was significant at 0.01 level (p=0.000). The results of the MANOVA test for gender are shown below in table 18 and 19.

Table 18. MANOVA test showing mean values for Gender

Estimates					
Dependent Variable	**Gender**			**95% Confidence Interval**	
		Mean	**Std. Error**	**Lower Bound**	**Upper Bound**
PTOT	F	62.983	.608	61.788	64.178
	M	62.044	.481	61.097	62.990
CSETOT	F	395.179	7.323	380.781	409.577
	M	433.710	5.800	422.306	445.113

Table 19. MANOVA test for Gender showing pair wise comparisons

Pair wise Comparisons							
Dependent Variable	**(I) Gender**	**(J) Gender**	**Mean Difference (I-J)**	**Std. Error**	**Sig.[a]**	**95% Confidence Interval for Difference[a]**	
						Lower Bound	**Upper Bound**
PTOT	F	M	.939	.775	.227	-.586	2.464
	M	F	-.939	.775	.227	-2.464	.586
CSETOT	F	M	-38.531*	9.342	.000	-56.897	-20.164
	M	F	38.531*	9.342	.000	20.164	56.897

Based on estimated marginal means

a. Adjustment for multiple comparisons: Least Significant Difference (equivalent to no adjustments).

*. The mean difference is significant at the .05 level.

The multivariate analysis of variances (MANOVA) was performed to compare means of dependent variables (PTOT and CSETOT) for age groups. The results showed that the participants of age group of 50+ had the highest mean value of information privacy concerns (IPC) (64.949) and the age group of 18-25 had the lowest mean value of IPC (58.332). The differences of mean values of IPC between age groups of 18-25 and 50+ and between age groups of 18-25 and 26-50 were significant at 0.01 level (p=0.000); but the difference of mean values of IPC between age groups of 26-50 and 50+ was not significant (p=0.470). The participants of age group of 26-50 were found to have highest computer self-efficacy (CSE) mean value (432.303) and the participants of age group of 50+ were found to have the lowest CSE mean value (384.234). The differences of mean values of CSE between age groups of 18-25 and 50+ and between 26-50 and 50+ were found to be significant at 0.01 level (p=0.000). But the difference of mean value of CSE between age groups of 18-25 and 26-50 was not found to be significant (p=0.608). MANOVA test results showed that the age groups of 18-25 and 26-50 had similar

computer self-efficacy mean values; and the age group of 50+ had lower CSE mean value than other two age groups. The results of MANOVA test for age groups are shown below in table 20 and 21.

Table 20. MANOVA test for Age showing pair wise comparisons

Pair wise Comparisons							
Dependent Variable	**(I) Age**	**(J) Age**	**Mean Difference (I-J)**	**Std. Error**	**Sig.[a]**	**95% Confidence Interval for Difference[a]**	
						Lower Bound	**Upper Bound**
PTOT	18-25	26-50	-5.927*	.891	.000	-7.678	-4.176
		50+	-6.618*	1.001	.000	-8.585	-4.651
	26-50	18-25	5.927*	.891	.000	4.176	7.678
		50+	-.691	.955	.470	-2.568	1.186
	50+	18-25	6.618*	1.001	.000	4.651	8.585
		26-50	.691	.955	.470	-1.186	2.568
CSETOT	18-25	26-50	-5.510	10.732	.608	-26.608	15.589
		50+	42.556*	12.054	.000	18.858	66.255
	26-50	18-25	5.510	10.732	.608	-15.589	26.608
		50+	48.066*	11.501	.000	25.456	70.676
	50+	18-25	-42.556*	12.054	.000	-66.255	-18.858
		26-50	-48.066*	11.501	.000	-70.676	-25.456

*. The mean difference is significant at the .01 level.

Table 21. MANOVA test showing mean values for Age

Estimates					
Dependent Variable	**Age**			**95% Confidence Interval**	
		Mean	**Std. Error**	**Lower Bound**	**Upper Bound**
PTOT	18-25	58.332	.665	57.025	59.638
	26-50	64.259	.593	63.093	65.425
	50+	64.949	.748	63.479	66.420
CSETOT	18-25	426.793	8.007	411.052	442.534
	26-50	432.303	7.146	418.254	446.352
	50+	384.237	9.011	366.521	401.953

The result from the test of hypothesis 3 showed that there was no significant relationship between gender and information privacy concerns. The test of hypothesis 5 showed that there was significant relationship between gender and computer self-efficacy. There was no significant difference between male and female with respect to information privacy concerns, but male participants were found to have higher computer self-efficacy than female participants which made the differences in correlation between male and female. The correlation between computer self-efficacy and information privacy for male was significant and positive, but the correlation for female was not significant. Therefore, from the results of correlation analysis, the MANOVA test, and hypotheses testing it could be concluded that there was a difference in relationship between genders with respect to the relationship between information privacy concerns and computer self-efficacy.

The result from the test of hypothesis 2 showed that there was significant positive relationship between age groups and information privacy concerns. The result from the test of hypothesis 4 showed that there was a negative significant relationship between age

groups and computer self-efficacy. Older participants were found to have lower computer self-efficacy and higher information privacy concerns than younger participants. The Spearman rank-order tests showed that there were differences in correlation coefficients in both magnitude and significance among age groups. MANOVA tests also showed the differences in mean values for both CSETOT and PTOT among age groups. On the basis of these tests, it could be concluded that there were differences in relationships among age groups with respect to the relationship between information privacy concerns and computer self-efficacy.

Summary of Results

This chapter described the data collection method and statistical tests used for data analysis of this study. The results of tests of five null hypotheses and analyses of two research questions were presented

Data was collected using face-to-face interaction with the participants where the participants were asked to fill out the survey questionnaire. The survey instrument was developed by combining two previously validated instruments (the Computer Self-Efficacy scale developed by Marakas et al., 2007 & the Internet Users' Information Privacy Concerns scale developed by Malhotra et al., 2004). Prior to actual study, a pilot study was conducted with 36 subjects. The results from the pilot study showed that the participants took an average of 20 minutes to fill out the survey questions, the questions were clear, most of the participants understood the questions, only few participants asked questions on some survey questions, and both the scales had high value for internal consistency reliability (Cronbach's alpha > 0.7). For actual study, data was collected

from 415 participants. The monetary reward of $2 was not found to be an incentive to attract participants. People were willing to participate in filling out the survey questions only when they understood the purpose of the study; and when they were assured that their responses would be anonymous and no personal information would be collected. From pre-analysis data screening, 15 datasets were omitted from final data analyses due to missing data and outliers. Demographic data of the participants showed that 59.25% were male, 40.75% were female, 30.75% were of age 18-25, 38.5% were of age 26-50, and 30.75% were of age 50+. Graphical methods (histograms, P-P plots, and Q-Q plots) and the Shapiro-Wilk tests were used to test data for bivariate normality. The results showed that data for both computer self-efficacy and information privacy concerns were not normally distributed and were skewed to the left.

The Spearman rank-order nonparametric correlation test was used to test five null hypotheses. *Hypothesis 1 was rejected*. The relationship between computer self-efficacy and information privacy concerns was found to be positive and significant at 0.05 level (p=.0.01), and the magnitude was low ($\rho = 0.128$). With the increase of an individual's computer self-efficacy, her information privacy concerns increase. *Hypothesis 2 was rejected*. The relationship between information privacy concerns and age groups was found to be positive and significant at 0.01 level (p=0.000), and the magnitude was low ($\rho = 0.342$). *Hypothesis 3 was supported*. The relationship between gender and information privacy concerns was not significant at 0.05 level (p=0.505). Male and female participants did not have significant differences in information privacy concerns. Therefore, with the increase of age, information privacy concerns increase regardless of gender. *Hypothesis 4 was rejected.* The relationship between computer self-efficacy and

age groups was found to be negative and significant at 0.05 level (p=0.015), and the magnitude was low (ρ= -0.121). With the increase of age, computer self-efficacy decreases. Younger participants were found to have higher computer self-efficacy than older participants. *Hypothesis 5 was rejected.* The relationship between computer self-efficacy and gender was found to be negative and significant at 0.01 level (p=0.001), and the magnitude was low (ρ = -0.170). The negative value of correlation coefficient showed that male participants had higher computer self-efficacy than female participants.

The test result of hypothesis 1 provided answer to the first research question. The test of hypothesis 1 showed that there was a significant relationship between computer self-efficacy and information privacy concerns. The relationship was positive and the magnitude was low. With the increase of an individual's computer self-efficacy, her information privacy concerns increase. This validated the findings of White et al. (2008). White et al. also found significant relationship between computer self-efficacy and two components of information privacy concerns (collection and control – unauthorized secondary use of data). The IUIPC scale, used for this study, included these two components (collection, control).

To seek answers to the second research question, three methods were used: the first method was the Spearman rank-order test for correlation analysis between information privacy concerns (IPC) and computer self-efficacy (CSE) for each of the age groups and genders, the second method was the MANOVA test to compare means of IPC and CSE between genders and among age groups, and the third method was testing of hypotheses 2, 3, 4, and 5. From the results of correlation analyses, the MANOVA tests, and hypotheses testing it could be concluded that there were differences in relationship

between genders and among age groups with respect to their relationships between computer self-efficacy and information privacy concerns. This was a new knowledge added to the research related to the relationships between antecedents of information privacy concerns and computer self-efficacy.

Chapter 5

Conclusion, Implications, Recommendations, and Summary

Conclusions

Results of this study showed that there was a significant and positive relationship between computer self-efficacy and information privacy concerns; and there were differences between genders and among age groups (18-25, 26-50, and 50+) with respect to their relationship between computer self-efficacy and information privacy concerns. When an individual's computer self-efficacy increases, his/her information privacy concerns also increase.

The main goal of this study was to validate the work of White et al. (2008) by investigating their findings with a broader population and with updated measuring scales; and to extend their work by investigating differences among different age groups and between genders regarding information privacy concerns and their relationships with computer self-efficacy. White et al. investigated relationship between computer self-efficacy and four factors of concerns for information privacy (CFIP) (*collection of data, errors, unauthorized secondary use, and improper access to data*). They used measuring scales that did not reflect today's computing technology like windows, spreadsheet, database, and Internet. Their study sample consisted of 82 undergraduate students. The sample size for this study was increased from 82 to 400. The study participants were chosen from broad population spread across different age groups and genders (30.75%

from ages of 18-25, 38.5% from ages of 26-50, 30.75% from ages of 50+, 59.25% from male, and 40.75% from female). This study used updated measuring scales that reflected current technology. For assessing information privacy concerns, the three-dimensional (*collection, control, awareness*) measuring scale of the Internet Users' Information Privacy Concerns (IUIPC), developed by Malhotra et al. (2004) was used. This was an updated CFIP scale with an additional dimension (*awareness*) to measure privacy concerns of Internet users. For assessing computer self-efficacy, six-dimensional *(general, windows, spreadsheet, word processing, Internet, and database*) measuring scale of the Computer Self-Efficacy Scale (CSES), developed by Marakas et al. (2007) was used. This scale adhered to the base theory of general computing and measured skills of current technology.

This study addressed two research questions, which were based on three specific goals of this study. The first research question was based on first specific goal of this study which was to empirically investigate relationship between computer self-efficacy (CSE) and information privacy concerns (IPC). The results showed that there was a significant and positive relationship between CSE and IPC. When an individual's computer self-efficacy increases, her information privacy concerns also increase. But the magnitude of this relationship was found to be low. This finding validated and strengthened previous findings by White et al. (2008). White et al. found that there were significant relationships between computer self-efficacy and two of factors of information privacy concerns – namely, collection of data and control of unauthorized secondary use of personal data. The IUIPC scale included these components. So, the results of this study validated findings by White et al. (2008). In addition, the results of this study found

significant relationship between computer self-efficacy and information privacy concerns with combined factors of all three components (collection, control, and awareness). White et el. did not investigate the correlation between CSE and IPC with combined factors.

The second research question was based on second and third specific goals of this study. The second specific goal of this study was to investigate correlation difference between CSE and IPC among different age groups. The third specific goal of this study was to investigate correlation difference between CSE and IPC between genders. The results from the correlation analyses, the MANOVA tests, and hypotheses tests showed that there were differences between genders and among age groups with respect to their relationships between computer self-efficacy and information privacy concerns. This finding further extended White et al. (2008)'s work. The results also showed that older Internet users were more concerned about information privacy than younger users and there were no significant differences between genders with respect to information privacy concerns. The findings of the influence of age and genders on information privacy concerns from this study supported the findings of Zukowski and Brown (2007). The results also showed that male participants had higher computer self-efficacy than female participants, the age group of 50+ had the lowest computer self-efficacy, and other two age groups (18-25 and 26-50) had similar computer self-efficacy (difference of means was not significant)

A possible explanation of why the results showed a significant and positive correlation between CSE and IPC may be the locus of control and awareness. Confidence with use and knowledge of computing technology makes people more aware of lack of

control of security and unauthorized use of their personal information. More they are aware of technology, more they are concerned about privacy of their personal information collected over the Internet.

Implications for Research and Practice

Understanding consumers' concerns regarding information privacy is important to researchers and practitioners. The implications of this study for the research are significant. This study contributed to the body of knowledge about the relationships between antecedents and consequences of information privacy concerns and computer self-efficacy. It had validated and extended work of White et al. (2008) by investigating relationship between computer self-efficacy and information privacy concerns with a broader population and with updated measuring scales, and also by adding new knowledge about the influence of age and gender on the correlation of computer self-efficacy and information privacy concerns. This study also addressed instrumentation issues in the information privacy and computer self-efficacy research by validating information privacy concerns instrument developed by Malhotra et al. (2004) and computer self-efficacy scale developed by Marakas et al. (2007). Researchers can use these instruments with increased confidence due to the results of this study which indicated acceptable reliability and validity.

The implications of this study for practitioners are twofold. The first implication is that the findings of this study can help corporations to improve e-commerce by targeting privacy policy-making efforts to address the explicit areas of consumer privacy concerns. The second implication is that the results of the study can help Information

Technology practitioners to develop privacy protection tools and processes and target those tools to specific consumer groups to address their privacy concerns.

Recommendations for Future Research

The target population of this study was the residents of the state of New Jersey. In order to generalize the findings, additional study with participants from multiple states or from multiple countries is recommended. This study investigated influence of gender and age on the correlation of computer self-efficacy and information privacy concerns. To further improve our understanding of the relationships of antecedents of information privacy concerns and computer self-efficacy, future research may focus on the influence of other demographic factors like education, income, and Internet experience on the correlation between computer self-efficacy and information privacy concerns. Consumers are concerned about identity theft and security of their personal information. Future research should use measuring scales that include concerns for identity theft and data security. As the computing technology changes over time, for future research, it may be essential to update items in computer self-efficacy and information privacy concerns scales to reflect the shift in the computing technology.

Summary

The research problem that this study addressed was the relationship between an individual's computer self-efficacy and her information privacy concerns and the differences among different age groups and between different genders regarding information privacy concerns and their relationships with computer self-efficacy.

Consumers' privacy concerns are complex and if they are not understood and mitigated, they can have negative consequences on e-commerce growth and Internet purchases (Malhotra, Kim, & Agarwal, 2004; Metzger, 2004; Phelps, Nowak, & Ferrel, 2000; Anton, Earp, He, Stufflebam, Bolchini, & Jensen, 2004). Computer self-efficacy has been shown to be an effective predictor of behavior intention (Ball, 2008) and a critical determinant of intention to use Information Technology (Compeau & Higgins, 1995; Marakas, Yi, & Johnson, 1998). White, Shah, Cook, and Mendez (2008) studied the relationship between computer self-efficacy and four factors of information privacy concerns (collection of data, errors in collecting data, unauthorized secondary use, and improper access to data) defined by Smith, Milberg, and Burk (1996). White et al. (2008) found that two factors of information privacy concerns (collection of data and unauthorized secondary use) had significant relationships with computer self-efficacy. Smith et al. (1996)'s privacy components addressed information privacy concerns related to corporate management of personal information and did not address Internet users' information privacy concerns. White et al. (2008) did not study the relationship between computer self-efficacy and information privacy concerns with all factors combined. Their study population was 82 undergraduate students and, therefore, the results lacked external validity. White et al. (2008) stressed the need to validate their work with a broader population and with updated measuring instruments that would reflect today's computing technology. They also emphasized the need to investigate the differences between genders and among different age groups with respect to their relationships between computer self-efficacy and information privacy concerns.

The main goal of this study was to validate the work of White et al. (2008) by investigating their findings with a broader population and with updated measuring scales; and to extend their work by investigating differences among different age groups and between genders regarding information privacy concerns and their relationships with computer self-efficacy. In addition, this study addressed three specific goals. The first specific goal of this study was to empirically investigate relationship between computer self-efficacy (CSE) and information privacy concerns (IPC) with a broader population (different age groups and genders) and updated scales to reflect current technology. The second specific goal of this study was to investigate correlation differences between CSE and IPC among different age groups. The third specific goal of this was to investigate correlation differences between CSE and IPC between genders. To address the research problem, a conceptual research model was developed (see Figure 1) and two research questions were formulated. The first research question was based on first specific goal and the second research question was based on second and third specific goals of this study. To seek answers to the research questions, five null hypotheses were developed. In order to address research questions and null hypotheses, a 63-item paper-based survey instrument was developed by combining two validated scales from the previous research. The survey instrument also contained demographic data like gender, age, and professional status. The survey instrument is shown in Appendix C. Data was collected through face-to-face interaction with the participants in various places like indoor shopping areas, social gatherings, places of worships, and college campuses, where participants were asked to fill out the survey questions. Prior to the actual study, a pilot study was conducted with 36 subjects. The results from the pilot study showed high

reliability coefficients (Cronbach's alpha > 0.7) for both the instruments (see Table 4), the questions were clear to the participants, and the participants took an average of 20 minutes to fill out the survey questions. The target population of this study was the randomly selected residents of the state of New Jersey, U.S.A over 18 years of age. Data for the actual study was collected from 415 participants over a period of 2 months (July-August, 2010). From pre-analysis of data screening, 15 participants were omitted due to missing data and outliers. Four hundred data items were used for final study. The demographic data was shown in table 8. Information privacy concerns were measured by adding Likert scale scores of all 10 items of IUIPC scale and computer self-efficacy was measured by adding Likert scale scores of all 53 items of CSES scale. The MS Excel and the Statistical Package for Social Science (SPSS) version 18 for windows were used for data preparation and data analysis. Data analysis included descriptive statistics, bivariate analysis for data normality, correlation analysis for testing hypotheses, and analysis of research questions. The result of the descriptive statistics was shown in table 9. Several graphical methods (histograms, P-P plots, Q-Q plots, and scatterplot) and the Shapiro-Wilk tests were used for bivariate data normality analysis. The results showed that data for both computer self-efficacy and information privacy concerns were not normally distributed. Therefore, nonparametric correlation analysis using the Spearman rank-order test was used to test five null hypotheses.

The results from hypotheses testing showed that only hypothesis 3 was supported and all other hypotheses were rejected (see Table 16). The hypothesis 1 addressed the first research question. The correlation analysis between computer self-efficacy (CSE) and information privacy concerns (IPC) showed that there was a positive and significant

relationship between CSE and IPC. For analysis of the second research questions, three test methods were used: testing of hypotheses 2-5, correlation analysis using the Spearman rank-order for each of the genders and age groups, and multivariate analysis of variance (MANOVA) tests for comparing means of CSE and IPC between genders and among age groups. The results of these tests showed that there were differences between genders and among age groups regarding relationships between CSE and IPC.

Despite the limitations mentioned earlier, this study met all goals of this study. The results validated and extended work of White et al. (2008). The results also added new knowledge about the influence of age and gender on the correlation between computer self-efficacy and information privacy concerns. The findings of this study would help corporations to improve e-commerce by targeting privacy policy-making efforts to address consumer privacy concerns. Finally, this research provided foundation for future research which could extend the knowledge in the area of information privacy concerns and computer self-efficacy research.

Appendix A

Summary of Privacy Concern Studies

Study	Method	Sample	Findings
Westin, 1967	Theoretical	Not applicable	Proposed a privacy topology and categorized privacy concerns into three groups: privacy fundamentalists (extremely concerned about privacy), privacy unconcerned (not concerned about privacy), and privacy pragmatists (are concerned, but less than fundamentalist).
Culnan, 1995	Survey	1991-Harris-Equifax consumer survey	Consumers who were unaware of name removal were more likely to be young, not well-educated, and to be African-American and are less likely to be concerned about privacy than consumers who are aware of name removal procedures.
Graubert & Coleman, 1999	Theoretical	Not applicable	Since the Internet is global in nature, the issue of privacy protection has an international dimension. While the government involvement and self-regulatory program were necessary to address the privacy concerns, the most effective way to protect the privacy of online users might ultimately come from high-tech marketplace itself.
Pippin, 1999	Theoretical	Not applicable	Internet is an under-regulated

Summary of Privacy Concern Studies (continued)

Study	Method	Sample	Findings
			commercial tool which allows collecting personal information and that information can be accessed by anyone. The United States does not have a privacy law that covers all consumers in the collection of personal data on-line.
Sheehan, 1999	Survey	889 online users	The results showed that women were more concerned about their personal privacy than men and men were more likely to adopt behavior to protect their privacy than women.
Milne & Rohm, 2000	Survey	1396 households	Consumers were neither aware of data collection efforts nor knowledgeable of name removal mechanisms. They were most likely to desire removal of their names from telephone list compared with email or mail list.
Miyazaki & Fernandez, 2000	Survey	160 Internet Users	For Websites with online shopping, a positive relationship exists between the privacy and security-related statements
Phelps et al., 2000	Survey	1500 catalog users	Consumers who were concerned with privacy, believed that there should be limit on how much information companies could collect.

Summary of Privacy Concern Studies (continued)

Study	Method	Sample	Findings
Dhillon & Moores, 2001	Experimental	27 experts	Identified five Internet privacy concerns: potential for companies to sell personal information (PI) to third party, lack of adequate security to protect PI from stealing, chance of losing PI, security of PI from being destroyed, and spam.
Miyazaki & Fernandez, 2001	Survey	160 Internet Users	Higher levels of Internet experience might lead to lower risk perceptions regarding online shopping and fewer concerns regarding system security; and more concerns regarding online privacy.
Phelps et al., 2001	Survey	1000 households	The consumers' attitude towards direct marketing and their desire for control over their personal information acts as antecedents to privacy. As privacy concern increases, purchase behavior decreases.
Stuart & Segars, 2002	Survey	355 consumers	Examined four dimensions of CFIP (collection, errors, secondary use, and unauthorized access) and found that consumers privacy concerns were multi-dimensional.

Summary of Privacy Concern Studies (continued)

Study	Method	Sample	Findings
Chen & Rea, 2004	Survey	160 students	The male users were more likely to falsify their personal information than female users. African American and Caucasians were less likely to falsify their personal information than other racial group (Asians and Hispanics).
Nwosu, 2004	Survey	7491 Internet users	Consumers were concerned about the security and privacy of their personal information and they were more inclined to shop online if they were assured of the security and privacy of their personal information.
Mollick, 2005	Experimental	84 students	Three privacy policy variables (informed consent, limiting data sharing within organizational boundary, and limiting unauthorized secondary use of data) could influence customers' perception of fairness and trustworthiness of an online firm.
Castaneda & Montoro, 2007	Survey	440 students	Customer's privacy concern of disclosing personal data had the most negative effect on the user's behavior on the Internet. The control over the collected information had a weak positive impact on the disclosure of personal information.

Summary of Privacy Concern Studies (continued)

Study	Method	Sample	Findings
Dolnicar & Jordaan, 2007	Survey	1855 households	Privacy concerns were associated with specific privacy-related behaviors - both actively protective behaviors (requesting deletion of personal information from the company's database) and passively protective behaviors (avoiding shopping over telephone).
Zukowski & Brown, 2007	Survey	200 professionals	The age had a definite influence on IUIPC. As the age of an Internet user increases, so does her level of privacy concern. The gender had no influence on IUIPC.
White et al., 2008	Survey	82 students	The individual with higher computer self-efficacy was less concerned with the collection of personal data; and was more concerned with unauthorized secondary use of personal data.
Zviran, 2008	Survey	217 students	Users with higher degree of privacy concerns were more cautious in their Web activities than users with lower degree of privacy concerns.

Summary of Privacy Concern Studies (continued)

Study	Method	Sample	Finding
Dinev et al., 2009	Survey	218 students	Perceived control was found to be the key factor influencing privacy perceptions in users' interaction with Web 2.0 related sites.

Appendix B

Summary of Computer Self-Efficacy Studies

Study	Method	Sample	Findings
Hill et al., 1987	Survey	304 students	The efficacy beliefs can sufficiently affect individual's decision in adopting technological Products and prior experience with computers does not affect subsequent behavior regarding further use of computer technology.
Tam, 1996	Experimental	15-week software training	Computer self-efficacy was a significant predictor of computer skills learning for people with physical disabilities.
Marakas et al., 1998	Theoretical	prior research works	Provided a thorough review of literature and conceptualized the multi-dimensional nature of computer self-efficacy (CSE). They theorized that CSE exists at both the general computing behavior level and at the specific computer task or application level.
Thatcher & Perrewe, 2002	Survey	211 students	Higher level of CSE caused low level of computer anxiety and low level of CSE caused high level of computer anxiety.

Summary of Computer Self-Efficacy Studies (continued)

Study	Method	Sample	Findings
Pearson, 2003	Survey	352 knowledge	Teamwork and information flow of an organization had a significant contribution to employees' computer self-efficacy. Involvement and supervision were found to have a negative relationship with an employees' computer self-efficacy. The meeting, climate and morale did not significantly contribute to computer self-efficacy.
Fagan et al., 2004	Survey	978 students	The experience, usage, and support of computer technology was positively related to computer self-efficacy, and anxiety was negatively related to computer self-efficacy.
Reed et al., 2005	Experimental	109 participants	There was a negative relationship between CSE and age. Differences in cognitive processes, memory, learning style, and less exposure to computer technology might have inhibited older workers' abilities to use computer technology.
Crossler & Belanger, 2006	Survey	36 students	CSE significantly affected a person's use of security tool; and instruction was not effective at increasing CSE and use of security tool.
Ndubisi, 2006	Survey	133 customers	CSE had a significant effect on the relationship between perceived usefulness,

Summary of Computer Self-Efficacy Studies (continued)

Study	Method	Sample	Findings
			perceived ease of use and intention of Internet banking.
Ball, 2008	Survey	59 instructors	Computer self-efficacy was the most significant contributing factor predicting behavioral intention to use technology.
Huai, 2008	Survey	258 teachers	CSE had a strong positive effect on perceived ease of use and intention of use of overhead projectors for class room teaching.
Reid, 2008	Survey	374 banking customers	CSE did not significantly predict customers' trust and perceived ease of use of banking system; but it significantly predicted perceived usefulness and perceived usefulness was a significant predictor of customers' attitudes and intentions to use banking system.
Robinson, 2008	Survey	258 students	CSE was found to be a significant predictor of intent to take additional online courses.
Urreta, 2008	Survey	323 students	CSE was found to have a positive and significant impact on performance in computer-supported tasks.
Ferdousi, 2009	Survey	119 instructors	CSE was found to be a key predictor of instructors' intention to use e-learning system

Appendix C

Survey Instrument

Please provide some general characteristic about you and circle the appropriate number for each item.

Gender: 1. Male 2. Female

Age: 1. 18-25 2. 26-50 3. Over 50

Professional status:

1. Students
   a. Undergraduate b. Graduate
2. Professionals
3. Retired

Please circle the number 1 to 10 where 1 is "Not at All Confident" to 10 "Totally Confident" with each item.

Item	Not at All Confident									Totally Confident
	1	2	3	4	5	6	7	8	9	10
CSEG1. I believe I have the ability to describe how a computer works.	1	2	3	4	5	6	7	8	9	10
CSEG2. I believe I have the ability to install new software applications on a computer.	1	2	3	4	5	6	7	8	9	10
CSEG3. I believe I have the ability to identify and correct common operational problems with a computer.	1	2	3	4	5	6	7	8	9	10
CSEG4. I believe I have the ability to unpack and set up a new computer.	1	2	3	4	5	6	7	8	9	10
CSEG5. I believe I have the ability to remove information from a computer that I no longer need.	1	2	3	4	5	6	7	8	9	10

Item	Not at All Confident					Moderately Confident				Totally Confident
	1	2	3	4	5	6	7	8	9	10
CSEG6. I believe I have the ability to understand common operational problems with a computer.	1	2	3	4	5	6	7	8	9	10
CSEG7. I believe I have the ability to use a computer to display or present information in a desired manner.	1	2	3	4	5	6	7	8	9	10
CSEW8. I believe I have the ability to group programs together using Windows.	1	2	3	4	5	6	7	8	9	10
CSEW9. I believe I have the ability to change system settings using Windows.	1	2	3	4	5	6	7	8	9	10
CSEW10. I believe I have the ability to create an icon for a program.	1	2	3	4	5	6	7	8	9	10
CSEW11. I believe I have the ability to delete an icon that I do not need.	1	2	3	4	5	6	7	8	9	10
CSEW12. I believe I have the ability to arrange icons so that I can conveniently access them.	1	2	3	4	5	6	7	8	9	10
CSEW13. I believe I have the ability to copy/move a file using Windows.	1	2	3	4	5	6	7	8	9	10
CSEW14. I believe I have the ability to change the appearance of Windows.	1	2	3	4	5	6	7	8	9	10
CSEW15. I believe I have the ability to delete a file that I do not need using Windows.	1	2	3	4	5	6	7	8	9	10
CSEW16. I believe I have the ability to change time and date of computer systems.	1	2	3	4	5	6	7	8	9	10
CSEW17. I believe I have the ability to change monitors settings using Windows.	1	2	3	4	5	6	7	8	9	10

Item	Not at All Confident							Moderately Confident		Totally Confident
	1	2	3	4	5	6	7	8	9	10
CSES18. I believe I have the ability to manipulate the way a number appears in a spreadsheet.	1	2	3	4	5	6	7	8	9	10
CSES19. I believe I have the ability to use and understand the cell references in a spreadsheet.	1	2	3	4	5	6	7	8	9	10
CSES20. I believe I have the ability to enter numbers into a spreadsheet.	1	2	3	4	5	6	7	8	9	10
CSES21. I believe I have the ability to use a spreadsheet to communicate numeric information to others.	1	2	3	4	5	6	7	8	9	10
CSES22. I believe I have the ability to write a sample formula in a spreadsheet to perform mathematical calculations.	1	2	3	4	5	6	7	8	9	10
CSES23. I believe I have the ability to summarize numeric information using a spreadsheet.	1	2	3	4	5	6	7	8	9	10
CSES24. I believe I have the ability to use a spreadsheet to share numeric information with others.	1	2	3	4	5	6	7	8	9	10
CSES25. I believe I have the ability to use spreadsheet to display numbers as graph.	1	2	3	4	5	6	7	8	9	10
CSES26. I believe I have the ability to use a spreadsheet to assist me in making decisions.	1	2	3	4	5	6	7	8	9	10
CSEWP27. I believe I have the ability to move a block of text using a word processor.	1	2	3	4	5	6	7	8	9	10
CSEWP28. I believe I have the ability to manipulate the way a paragraph looks using a word processor.	1	2	3	4	5	6	7	8	9	10

Item	Not at All Confident					Moderately Confident				Totally Confident
	1	2	3	4	5	6	7	8	9	10
CSEWP29. I believe I have the ability to add a footnote to a document using a word processor.	1	2	3	4	5	6	7	8	9	10
CSEWP30. I believe I have the ability to merge information from two documents using a word processor.	1	2	3	4	5	6	7	8	9	10
CSEWP31. I believe I have the ability to insert and delete words in a paragraph using a word processor.	1	2	3	4	5	6	7	8	9	10
CSEWP32. I believe I have the ability to change the appearance of words or phrases within a paragraph using a word processor.	1	2	3	4	5	6	7	8	9	10
CSEWP33. I believe I have the ability to check or improve my grammar in a document using a word processor.	1	2	3	4	5	6	7	8	9	10
CSEI34. I believe I have the ability to create a shortcut to access programs.	1	2	3	4	5	6	7	8	9	10
CSEI35. I believe I have the ability to download the information from another computer to my computer using the Internet.	1	2	3	4	5	6	7	8	9	10
CSEI36. I believe I have the ability to connect to another computer using the Internet.	1	2	3	4	5	6	7	8	9	10
CSEI37. I believe I have the ability to subscribe to a newsgroup.	1	2	3	4	5	6	7	8	9	10
CSEI38. I believe I have the ability to transfer files from my computer to another computer using the Internet.	1	2	3	4	5	6	7	8	9	10
CSEI39. I believe I have the ability to locate information on another computer using the Internet.	1	2	3	4	5	6	7	8	9	10
CSEI40. I believe I have the ability to send messages to others using the Internet.	1	2	3	4	5	6	7	8	9	10

Item	Not at All Confident			Moderately Confident						Totally Confident
	1	2	3	4	5	6	7	8	9	10
CSEI41. I believe I have the ability to publish information on the Internet.	1	2	3	4	5	6	7	8	9	10
CSEI42. I believe I have the ability to move from one computer to another using the Internet.	1	2	3	4	5	6	7	8	9	10
CSEI43. I believe I have the ability to navigate through Internet sites.	1	2	3	4	5	6	7	8	9	10
CSED44. I believe I have the ability to specify a primary key using a database program.	1	2	3	4	5	6	7	8	9	10
CSED45. I believe I have the ability to communicate information using a database program.	1	2	3	4	5	6	7	8	9	10
CSED46. I believe I have the ability to update the database using a database program.	1	2	3	4	5	6	7	8	9	10
CSED47. I believe I can create a query using a database program.	1	2	3	4	5	6	7	8	9	10
CSED48. I believe I have the ability to create a database table using a database program.	1	2	3	4	5	6	7	8	9	10
CSED49. I believe I have the ability to understand a query written in a database program.	1	2	3	4	5	6	7	8	9	10
CSED50. I believe I have the ability to create a field using a database program.	1	2	3	4	5	6	7	8	9	10
CSED51. I believe I have the ability to summarize information from database table using a database program.	1	2	3	4	5	6	7	8	9	10
CSED52. I believe I have the ability to add or delete a specific record from a database using a database program.	1	2	3	4	5	6	7	8	9	10
CSED53. I believe I have the ability to manipulate the information in a field using a database program.	1	2	3	4	5	6	7	8	9	10

Please circle the number 1 to 7 where 1 is "Strongly Disagree" to 7 "Strongly Agree" with each item.

Item	Strongly Disagree			Neutral			Strongly Agree
	1	2	3	4	5	6	7
PCON1. Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.	1	2	3	4	5	6	7
PCON2. Consumer control of personal information lies at the heart of consumer privacy.	1	2	3	4	5	6	7
PCON3. I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.	1	2	3	4	5	6	7
PAW4. Companies seeking information online should disclose the way the data is collected, processed, and used.	1	2	3	4	5	6	7
PAW5. A good consumer online privacy policy should have a clear and conspicuous disclosure.	1	2	3	4	5	6	7
PAW6. It is very important for me that I am aware and knowledgeable about how my personal information will be used.	1	2	3	4	5	6	7
PCOL7. It usually bothers me when online companies ask me for personal information.	1	2	3	4	5	6	7
PCOL8. When online companies ask me for personal information, I sometimes think twice before providing it.	1	2	3	4	5	6	7
PCOL9. It bothers me to give personal information to so many online companies.	1	2	3	4	5	6	7
PCOL10. I am concerned that online companies are collecting too much personal information about me.	1	2	3	4	5	6	7

Appendix D

IRB Approval from Nova Southeastern University

NOVA SOUTHEASTERN UNIVERSITY
Office of Grants and Contracts
Institutional Review Board

MEMORANDUM

To: Mohammad Awwal

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

Date: June 25, 2010

Re: *An Investigation of Factors that Affect HIPAA Security Compliance in Academic Medical Centers*

IRB Approval Number: wang06151002

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: *inga@nsu.nova.edu* • Web site: www.nova.edu/cwis/ogc

Appendix E

IRB Approval from Rider University

RIDER UNIVERSITY
College of Business Administration

2083 Lawrenceville Road
Lawrenceville, NJ 08648-3099
T 609-896-5152
F 609-896-5255
www.rider.edu

5/28/2010

To Whom It May Concern at Nova Southeastern University:

I am writing as the College of Business Administration representative to Rider University's Institutional Review Board. I understand that as part of his doctoral dissertation study, Mohammad Awwal is studying the relationship between college student age individuals' computer self-efficacy and privacy concerns. I have reviewed his materials, and have approved his use of Rider University College of Business Administration students in data collection.

If I can be of any further assistance, please do not hesitate to contact me at ekutcher@rider.edu.

Sincerely,

Eugene J. Kutcher III

Assistant Professor
Department of Management and Human Resources
College of Business Administration
Rider University

Appendix F

Permission Letter from Menlo Park Mall

SIMON MALLS | more choices®

MENLO PARK MALL

May 8, 2010

Mohammad Awwal
Doctoral Student, Nova Southeastern University
22 Cummings Rd
Monmouth Junction
NJ 08852

Dear Mohammad:

From the information you presented and the discussion of your research topic and survey plans, I feel that we have a good understanding of your research work. Permission is granted for you to conduct your research at Menlo Park Mall. Date to be determined and followed up with contract, insurance and payment.

There is no special requirement or restrictions placed on your research except that we will be allowed to review your final survey before it is implemented and we will be notified the date and time of starting of the survey and date and time of ending the survey. Designated location on mall will be presented at time of contract agreement.

Sincerely,

Suzy Lichter
Area Marketing Director
Menlo Park Mall

100 Menlo Park, Suite 500, Edison, NJ 08837
732-549-1900 | fax 732-549-9370 | www.simon.com

Reference List

Adomavicius, G., & Tuzhilin, A. (2005). Personalization technologies: a process-oriented perspective. *Communications of the ACM*, 48 (10), 83-90.

Anton, A.I., Earp, J.B., He, Q., Stufflebam, W., Bolchini, D., & Jensen, C. (2004). Financial Privacy policies and the need for Standardization. *IEEE Security & Privacy*, 2(2), 36-45.

Ball, D.M. (2008). An empirical Investigation of the contribution of Computer Self-Efficacy, Computer Anxieties, and Instructors' Experience with the Use of Technology to Their Intention to Use Emerging Educational Technology in Traditional Classrooms *Dissertations and Theses*. (Publication No. AAT 3297720).

Bandura, A. (1977). Self-efficacy: Toward a Unifying Theory of Behavioral Change. *Psychological Review*, 84 (2), 191-215.

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Englewood Cliffs, NJ: Prentice Hall.

Bandura, A., & Wood, R.E. (1989). Effect of perceived controllability and performance standards on self-regulation of complex decision-making. *Journal of Personality and Social Psychology*, 56 (5), 805-814.

Barlett, J.E., Kotrlik, J.W., & Higgins, C.C. (2001). Organizational Research: Determining Appropriate Sample Size in Survey Research. *Information Technology, Learning, and Performance Journal*, 19(1), 43.

Blanke, S. J. (2008). A Study of the Contributions of Attitude, Computer Security Policy Awareness, and Computer Self-Efficacy to the Employees' Computer Abuse Intention in Business Environments. *Dissertations and Theses*. (Publication No. AAT 3336919).

Buchanan, T., Pain, C., Joinson, A.N., & Reips, U. (2007). Development of measures of Online Privacy Concern and Protection for Use on the Internet. *Journal of the American Society for Information Science and Technology*, 58(2), 157-165.

Castaneda, J.A. & Montoro, F.J. (2007). The effect of Internet general privacy concern on customer behavior. *Electronic Commerce Research*, 7 (2), 117-141.

Chellappa, R.K. & Sin, R.G. (2005). Personalization versus Privacy: An Empirical Examination of other Online Consumers' Dilemma. *Information Technology and Management*, 6, 181-202.

Chen, K. & Rea, A.I. (2004). Protecting Personal Information Online: A survey of User Privacy Concerns and Control Techniques. *The Journal of Computer Information Systems*, 44(4), 85.

Compeau, D.R., & Higgins, C.A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, 19(2), 189-211

Compeau, D.R., & Higgins, C.A. (1995a). Application of social cognitive theory to training for computer skills. *Information Systems Research*, 6(2), 118-143.

Crossler, R. E. and Bélanger, F. (2006).The effect of computer self-efficacy on security training effectiveness. In *Proceedings of the 3rd Annual Conference on information Security Curriculum Development* (Kennesaw, Georgia, September 22 - 23, 2006).

Culnan, M.J. (1995). Consumer Awareness of Name Removal Procedures: Implication for Direct Marketing. *Journal of Direct Marketing*, 9 (2), 10-19.

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

Davis, F.D. (1986). A Technology Acceptance Model for Testing New End-User Information. *Dissertations and Theses*. (Publication No. AAT 0374529).

Dhillon, G.S. & Moores, T.T. (2001). Internet Privacy: Interpreting Key Issues. *Information Resources Management Journal*, 14 (4), 33-37.

Dinev, T. & Hart, P. (2004). Internet privacy concerns and their antecedents – measurement validity and a regression model. *Behaviour & Information Technology*, 23(6), 413-422.

Dinev, T. & Hart, P. (2006a). Privacy Concerns and Levels of Information Exchange: An Empirical Investigation of Intended e-Services Use. *e-Service Journal*, 4(3), 25-59.

Dinev, T. & Hart, P. (2006b). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, 17(1), 61-80.

Dinev, T., Xu, H., & Smith, H.J. (2009). Information Privacy Values, Beliefs and Attitudes: An Empirical Analysis of Web 2.0 Privacy. *Proceedings of the 42nd Hawaii International Conference on System Sciences.*

Deng, X., Doll, W.J., & Truong, D. (2004). Computer self-efficacy in an ongoing use context. *Behaviour & Information Technology*, 23(6), 395-412.

Dolnicar, S. & Jordaan, Y. (2007). A market-oriented approach to responsibly managing information privacy concerns in direct marketing. *Journal of Advertising, 36 (2), 123-149*.

Fagan, M.H., Neil, S., & Wooldridge, B.R. (2004). An empirical investigation into the relationship between computer self-efficacy, anxiety, experience, support and usage. *The Journal of Computer Information Systems*, 44(2), 95-104.

Ferdousi, B.J. (2009). A Study of factors that Affect Instructor's Intention to Use E-Learning Systems in Two-Year Colleges. *Dissertations and Theses*. (Publication No. AAT 3352474).

Garfinkel, S. (2000). *Database nation: The death of privacy in the 21st century*. Cambridge: O'Reilly & Associates.

Graubert, J., & Coleman, J. (1999). Consumers protection and antitrust enforcement at the speed of light: The FTC Meets the Internet. *United States Law Journal*, 25, 275-293.

Heerwegh, D. & Loosveldt, G. (2008). Face-to-face versus web surveying in a high-Internet-coverage population: difference in response quality. *Public Opinion Quarterly*, 72 (5), 836-846.

Hill, T., Smith, N.D., & Mann, M.F. (1987). The Role of Efficacy Expectations in Predicting the Decisions to Use Advanced Technology: The Case of Computers. *Journal of Applied Psychology*. 77(2), 307-313.

Hornsby, J. (2007). An empirical Investigation of the Effects of Discounting on Privacy Related Decisions. *Dissertations and Theses*. (Publication No. AAT 3258698).

Huai, P.C. (2008). Computer Self-Efficacy and job relevance Analysis of Teacher Acceptance of Information Technology. *2008 International Workshop on education Technology and Training & 2008 International workshop on Geoscience and Remote sensing*, 640-644.

Johnson, R.D. & Marakas, G.M. (2000). The role of behavioral modeling in computer skills acquisition: Toward refinement of the model. *Information Systems Research*, 11(4), 403-417.

Kelly, E.P. (2000). Ethical aspects of managing customer privacy in electronic commerce. *Human Systems Management*, 19, 237-244.

King, C.V. (2008). Online Privacy and Security of Internet Digital Certificates: A Study

of the Awareness, Perceptions, and Understanding of Internet Users. *Dissertations and Theses* (UMI No. 3320814).

Kuechler, W., & Grupe, F.H. (2003). Privacy and security in e-business. Digital signatures: A business view. *Information Systems Management*, 20 (1), 19-28.

Kuo, F.Y. & Hsu, M.H. (2001). Development and Validation of Ethical Computer Self-Efficacy Measure: The Case of Soft lifting. *Journal of Business Ethics*, 32 (4), 299-315.

Laudon, K.C., & Traver, C. (2001). *E-Commerce: Business, Technology, Society*. Addison Wesley, Boston, MA.

Leidner, D.E., & Jarvenpaa, S.L. (1995). The use of information technology to enhance management school education: A theoretical view. *MIS Quarterly*, 19(3), 265-291.

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

Liang, X. (2005). Development and Validation of a new Computer self-efficacy scale for use in complex technology context. *Dissertations and Theses* (Publication No. AAT 3183891).

Luo, X., & Seyedian, M. (2004). Contextual marketing and customer-orientation strategy for e-commerce: An empirical analysis. *International Journal of Electronic Commerce, 8* (2), 95-118.

Malhotra, N.K., Kim, S.S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, 15 (4), 336-354.

Marakas, G.M., Yi, M.Y., & Johnson, R.D. (1998). The multifaceted character of computer self-efficacy: Toward clarification of the construct and an Integrative Framework for Research. *Information Systems Research*, 9 (2), 126-163.

Marakas, G.M., Johnson, R.D., & Clay, P.F. (2007). The Evolving Nature of the Computer Self-Efficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Overtime. *Journal of the Association of Information Systems*, 8(1), 16-46.

Martocchio, J.J. (1992). Microcomputer usage as an opportunity: The influence of context in employee training. *Personal Psychology*, 45(3), 529-552.

Martocchio, J.J. & Webster, J. (1992). Effects of feedback and cognitive

playfulness on performance in microcomputer software training. *Personal Psychology*, 45(3), 553-578

Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly, 10* (1), 5-12.

McClave, J.T., Benson, P.G., & Sincich, T. (2005*). Statistics For Business and Economics*. Upper Saddle River, NJ: Pearson Prentice Hall.

Mertler, C., & Vanatta, R. (2001). *Advanced and multivariate statistical methods: Practical application and interpretation.* Los Angeles: Pyrczak.

Metzger, M.J. (2004). Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce. *Journal of Computer Mediated Communication*. 9 (4). Retrieved December 7, 2010, from http://jcmc.indiana.edu/vol9/issue4/metzger.html

Miyazaki, A.D. & Fernandez, A. (2000). Internet Privacy and Security: An Examination of Online Retailer Disclosures. *Journal of Public Policy & Marketing,* 19 (1), 54-61.

Miyazaki, A.D. & Fernandez, A. (2001). Consumer Perception of Privacy and Security Risks for Online Shopping. *The Journal of Consumer Affairs,* 35 (1), 27-44.

Milne, G. R., & Rohm, A.J. (2000). Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives. *Journal of Public Policy & Marketing*, 19 (2), 238-249.

Mollick, J.S. (2005). Privacy Policies, Fairness, Trustworthiness, and Willingness to Transact with Firms Online. *Dissertations and Theses*. (Publication No. AAT 3204647).

Muris, T.J. (2001). Protecting Consumers' Privacy: 2002 and beyond. *The Privacy 2001 Conference*, Cleveland, October 4, Ohio. Retrieved December 7, 2010 from the http://www.ftc.gov/speeches/muris/privisp1002.htm

Murphy, C.A., Coover, D., & Owen, S.V. (1989). Development And Validation of the Computer Self-Efficacy Scale. *Education and Psychological Measurement*, 49 (4), 893-899

Nakos, J.D. (2003). Information Privacy Concerns and Information Practices. *Dissertations and Theses*. (Publication No. AAT 3100241).

Ndubisi, N.O. (2006). Customers' perceptions and intention to adopt Internet banking: The moderation effect of computer self-efficacy. *AI & Society*, 21(3), 315-328

Nunnally, J.C. & Bernstein, I.H. (1994). *Psychometric Theory (3rd Edition)*. McGraw-Hill Series in Psychology, McGraw-Hill, Inc., New York: NY, 264-265.

Nwosu, S.C. (2004). Effects of security and privacy concerns on online consumer purchase behavior. *Dissertations and Theses*. (Publication No. AAT 3159700).

O'Neil, D. (2001). Analysis of Internet Users' Level of Online Privacy Concerns. *Social Science Computer Review,* 19 (1), 17-31.

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

Phelps, J.E, D'Souza, D., & Nowak, G. (2001). Antecedents and consequences of consumer privacy concerns: an empirical investigation. *Journal of Interactive Marketing,* 15 (4), 2-17.

Pippin, R.K. (1999). Consumer privacy on the Internet: It's "surfer beware". *Air Force Law Review*, 47, 125-161.

Pirim, T., James, T., Boswell, K., Reithel, B., & Barkhi, R. (2008). An Empirical Investigation of an Individual's Perceived Need for Privacy and Security. *International Journal of Information Security and Privacy*, 2(1), 42-53.

Pollach, I. (2006). Privacy Statements as a Means of Uncertainty Reduction in WWW Interactions. *Journal of Organizational and End User Computing, 18(1), 23-49.*

Reed, K., Doty, D.H., & May, D.R. (2005). The impact of aging on self-efficacy and computer skill acquisition. *Journal of Managerial Issues*. 17(2), 212-228.

Reid, M. (2008). Integrating Trust and Computer Self-efficacy into the Technology acceptance Model: Their Impact on Customers' Use of Banking Information systems in Jamaica. *Dissertations and Theses*. (Publication No. AAT 3336438).

Richards, J.I. (1997). Legal Potholes on the Information Superhighway. *Journal of Public Policy & Marketing,* 16 (2), 319-326.

Robinson, D.L. (2008). Relationship of Student Self-Directedness, Computer Self-Efficacy, and Student Satisfaction to persistence in Online Higher Education Programs. *Dissertations and Theses*. (Publication No. AAT 3328226).

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

Sheehan, K.B. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing*, 13 (4), 24-38.

Sheehan, K.B., & Hoy, M.G. (1999). Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns. *Journal of Advertising*, 28 (3), 37-51.

Sheng, Y. & Pearson, M. (2003). Organizational Culture and Employees' Computer Self-Efficacy: an Empirical Study. *Information Resource Management Journal*, 16(3), 42-58.

Sheng, H., Nah, F.F., & Siau, K. (2008). An experimental Study on Ubiquitous commerce Adoption: Impact of Personalization and Privacy Concerns. *Journal of the Association for Information Systems*, 9(6), 344-376.

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

Stewart, K.A & Segars, A.H. (2002). An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research*, 13(1), 36-49.

Stone, E.F.D.G., Gardner, H.G., Gueutal, & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs and attitudes across several types of organizations. *Journal of Applied Psychology*, 68(3), 459-468.

Sun, F., Omachi, S., Kato, N., Aso, H., Kono, S., & Takagi, T. (2000). Two-stage computational cost reduction algorithm based on Mahalanobis distance approximations. *Proceedings of the 15th International Conference on Pattern Recognition (ICPR'00)*, 2, 2696.

Tam, S.F. (1996). Self-Efficacy as a Predictor of Computer Skills Learning Outcomes of Individuals With Physical Disabilities. *The Journal of Psychology*, 130 (1), 51-58.

Thatcher, J.B., & Perrewe, P.L. (2002). An empirical examination of individual traits as antecedents to computer anxiety and computer self-efficacy. *MIS Quarterly*, 26(4), 381-396.

Turban, E., Leidner, D., Mclean, E., & Wetherbe, J. (2008). *Information Technology for Management. Transforming Organizations in the Digital Economy*. 6th Edition. Hoboken, NJ: John Wiley & Sons, Inc.

Turner, E. C. & Dasgupta, S. (2003). Privacy on the Web: An examination of user concerns, technology, and implications for business organizations and individuals. *Information Systems Management*, 20 (1), 8-18.

Urreta, M.I. (2008). An Empirical investigation into the moderating relationship of computer self-efficacy on performance in a computer supported task. *Dissertations and Theses*. (Publication No. AAT 330950).

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

White, G.L., Shah, J.R., Cook, J.R., & Mendez, F. (2008). Relationship Between Information Privacy Concerns and Computer Self-Efficacy. *International Journal of Technology and Human Interaction*. 4(2), 52-82.

Zagorsky, J.l., & Rhoton, P. (2008). The effects of promised monetary incentives of attrition in a long term panel survey. *Public Opinion Quarterly*, 27 (3), 502-513.

Zhang, Y. & Espinoza, S. (1998). Relationships among Computer Self-Efficacy, Attitudes Toward Computers, and Desirability of Learning Computing Skills. *Journal of Research on Computing in Education*, 30 (4), 420-436.

Zukowski, T. & Brown, I. (2007). Examining the Influence of Demographic Factors on Internet Users' Information Privacy Concerns. *Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists (SAICSIT) on IT research in developing countries*. October, 2007. Fish River Sun, Sunshine Coast, South Africa.

Zviran, M. (2008). User's perspective on privacy in web-based applications. *The Journal of Computer Information Systems*, 48 (4), 97.