EMPIRICAL INVESTIGATION OF THE RELATIONSHIP OF PRIVACY, SECURITY AND TRUST WITH BEHAVIORAL INTENTION TO TRANSACT IN E-COMMERCE

by

ANIL GURUNG

Presented to the Faculty of the Graduate School of

The University of Texas at Arlington in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT ARLINGTON

May 2006

ACKNOWLEDGEMENTS

This dissertation would not have been completed without the support of my colleagues at the Department of Information Systems and Operations Management, UTA, who helped me with data collection. I would like to thank Anil Singh, David Weltman, George Mangalaraj, Jeyaraj Davamani, Karen Sarratt, Kishen Iyengar and Vishnu Vinekar for allowing me to take the survey in their classes.

I am very grateful for the excellent guidance of my chair, M. K. Raja, and to all the members of my committee, including Sandra C. Henderson, Sridhar Nerur, Mark Eakin and Patricia Swafford. Each member of the committee provided valuable insight at different stages of this research.

In addition to my committee members I would also like to thank Nancy A. Rowe for her assistance in early part of data analysis, and thanks to Alencia Aghayere, Anurag Jain, Irina G. Maximova and Pamela Broussard for proof-reading my dissertation.

Finally, no words of thanks are ever enough for the dedication of my parents and late grandmother who pushed me through each step of my academic journey and wanted to see me get the first doctorate in the family.

April 18, 2006

ABSTRACT

EMPIRICAL INVESTIGATION OF THE RELATIONSHIP OF PRIVACY, SECURITY AND TRUST WITH BEHAVIORAL INTENTION TO TRANSACT IN E-COMMERCE

Publication No. _____

Anil Gurung, PhD.

The University of Texas at Arlington, 2006

Supervising Professor: M. K. Raja

Privacy and security concerns of consumers have been touted as one of the hindrances in the growth of e-commerce. These concerns increase risk perception of consumers. Understanding the consequences of privacy and security concerns, and their relationship to risk perceptions may provide a solution. The relationship between privacy and security is investigated using the Theory of Planned Behavior. The model proposed in this study, investigates the relationship of trust, privacy and security concerns to the risk perception adoption of e-commerce. The results from a field study validate the model.

TABLE OF CONTENTS

LIST OF FIGURES

Figure **Page**

LIST OF TABLES

Table **Page**

CHAPTER 1

INTRODUCTION

1.1 Problem Statement

Privacy concerns of consumers make them hesitant to engage in electronic commerce (e-commerce) transactions which require them to divulge personal information; such as date of birth, social security number, home telephone number, and credit card information et cetera. Protecting consumers' privacy is an important factor for the success of e-commerce (Liu et al. 2004). However, gathering information about consumers is necessary for e-commerce, in order to gain a better understanding of consumer preferences. Therefore, managers face a challenging task in collecting necessary consumer information required to maximize sales and profits, without compromising privacy.

Privacy concerns of consumers have been well addressed in research (Culnan 1993; Hoffman et al. 1999b; Smith et al. 1996; Stewart and Segars 2002). One popularly used definition of privacy is "the right to be let alone", which quoted Judge Thomas Cooley's claim in extension to "right to life" (Warren and Brandeis 1890). "Right to life" is the common law regarding the right of individuals to have full protection in person and in property (Warren and Brandeis 1890). Privacy may have multiple dimensions such as privacy of an

individual's body, privacy of personal behavior, privacy of personal communication, and privacy of personal data (Clarke 1999). In marketing literature, invasion of privacy is interpreted as unauthorized collection, disclosure, or other use of personal information such as selling it to other e-marketers (Wang et al. 1998). It has been established that, generally, consumers are concerned about maintaining their privacy (Culnan and Armstrong 1999; Culnan 1993; Dinev and Hart 2003; Hoffman et al. 1999a; Smith et al. 1996). With sophisticated information technologies collecting information, the issue of information privacy has become more and more important as consumer advocates, public policy makers and companies debate possible ways to protect consumer privacy (Singh and Hill 2003). Henderson and Snyder (1999) summarize three main forces driving the importance of information privacy. They include new technological capabilities, increasing value of information and ethical issues.

The advent of technological capabilities such as Enterprise Resource Planning (ERP) and client-server systems allow companies to efficiently collect, store and exchange consumer data. Cookies and spyware are used to track consumer's actions on the web to get information about consumer behavior and preferences, sometimes, without consent or knowledge of the consumer (Olivero and Lunt 2004). Sophisticated data-mining tools make it easier to analyze consumer data. Data collected on consumer behavior and preferences

are used by companies to develop strategies for customer retention and market growth.

It has been noted that concerns for privacy may have been fueled by consumer awareness of the value of the collected information (Hagel and Rayport 1997). The value of information is also highlighted by the possible risk associated with misuse of information collected by companies, such as, unauthorized disclosure to third parties. Media coverage on privacy issues only serves to bolster privacy concerns.

Some of the information gathering practices by companies also raise privacy concerns. Use of covert techniques, such as spyware, poses additional threats to consumer privacy. The level of threat depends on the nature of Spyware. Many researchers have studied consumer attitudes to examine the effects of privacy concerns (Dinev and Hart 2003; Dommeyer and Gross 2003; Vijayasarathy 2004). In spite of these past studies, it is still unclear how privacy concerns actually impact consumer behavior.

To mitigate these privacy concerns, trust in online companies has been established as an important determinant of consumer behavior in the context of e-commerce (Liu et al. 2004; Luo 2002; Malhotra et al. 2004). Trust is an expectation on the part of consumers that the online company with which they engage in transactions, will not behave opportunistically by taking advantage of the situation (Gefen et al. 2003; McKnight et al. 2002a). Consumers perceive significant risks and uncertainty when dealing with online companies, because

of factors such as, uncertainty about vendor attributes and behavior, inability to inspect the product, inability to monitor the actions of the online company, privacy and security of personal information et cetera. In the absence of direct measures to control social complexity in an online environment, trust is often viewed as an important factor to reduce risk and uncertainty (Luhmann 1979).

Online companies seek to gain trust by the use of web seals on their websites. Web seals are approvals from a third-party showing that the website has met certain criteria for privacy and/or security policies. Trust in companies increases the likelihood that consumers will participate in e-commerce transactions (McKnight et al. 2002b). This implies that the perceived risks arising from privacy concerns decrease to some extent by having trust. Privacy research has studied the impact of various risks and benefits consumers assume while taking part in e-commerce (Jarvenpaa et al. 1999; Phelps et al. 2000). A consumer makes a calculation of risk, which can be attributed to some extent to his/her privacy concerns and the benefits of taking part in e-commerce, then reaches the decision as to whether or not to take part in the e-commerce transaction. Culnan and Bies (1999) proposed that consumers have a "privacy calculus" to weigh the potential risks and benefits of providing personal information in exchange for economic or social gains. Similarly, Dhillon et al. (2002) stated that consumers make "value-focused" privacy-based assessments about the firms when they transact. However, there has been little empirical evidence of how privacy and trust affects consumer behavior

1.2 Importance of the Study

Primarily, privacy and security concerns are treated as a single construct in most of the privacy literature (Liu et al. 2004; Xu and Teo 2004). Security concern is taken as one of the dimensions of the overarching privacy concerns. Belanger et al (2002) cite that privacy and security concerns should be conceptualized as distinct, and that there is a lack of understanding of their relations. Others agree, that, privacy and security concerns are two different constructs (Chang et al. 2005; Vijayasarathy 2004). In response to general sentiment, this study attempts to provide a clear delineation of the impact of privacy and security concerns as two distinct constructs.

Most studies on consumer privacy focus on establishing rules that help companies collect private information without compromising consumer satisfaction (Culnan and Armstrong 1999; Lunt 1999; Milne and Culnan 2002; Miyazaki and Fernandez 2000). Privacy concerns inherent in consumers motivate them to adopt strategies such as withholding personal information, or providing false information (Hoffman et al. 1999a; Pitkow and Kehoe 1997). Research indicates that consumers, despite their privacy concerns, are aware of the importance of consumer data and are interested in providing such information, whenever applicable, and when the conditions of full disclosure or informed consent are present (Culnan and Armstrong 1999; Hoffman et al. 1999a). Researchers have suggested that privacy concerns may be addressed through the use of fair information practices by providing consumers with more

control over their personal information and developing trust (Culnan and Armstrong 1999; Foxman and Kilcoyne 1993; Milne 2000; Phelps et al. 2000). Providing control over the use of information by adopting fair information practices may reduce the perceived risk associated with secondary information use, however, there is lack of evidence that informational control would lead to the development of trust (Olivero and Lunt 2004).

To develop an integrative framework of e-commerce adoption, the theory of planned behavior (TPB), as proposed by (Ajzen 1991), will be used in this study. TPB suggests that behavior is predicted by intention, and intention is formed by attitudes, subjective norm and perceived behavioral control. Attitudes, in their turn, are shaped by beliefs. The variable of interest for online companies is the willingness of consumers to transact in e-commerce. The objective of this study is to identify the factors that contribute to the willingness, or intention of consumers to transact in e-commerce and further study the relationship between those factors.

Another objective of this research is to study the relation between trust beliefs and risk perception. Mayer, Davis and Schoorman (1995) proposed a model of organizational trust that outlines conditions present when organizational trust occurs. The model posits the types of relationships and contexts in which trust has an effect. The contextual factors that affect trust are the stakes involved, the balance of power in the relationship, the level of risk perception, and the alternatives available to the trustor. Trust is inter-related

with risk (McAllister 1995). A consumer does not need to risk anything in order to trust; however, he/she must take a risk in order to engage in a trusting action or trust behavior (e.g. participate in e-commerce). The main difference between trust and trusting behavior is a “willingness” to assume risk and actually “assuming” risk. Risk perception refers to the “trustor’s belief about the likelihoods of gains or losses outside of considerations that involve the relationship with the particular trustee” (Mayer et al. 1995). The difference between trust behavior and risk behavior may be distinguished in terms of a “relationship” (Ruppel et al. 2003). Trust behavior involves risk-taking in a “relationship”, whereas risk behavior “may not involve relationships”. The presence of a “prior relationship” helps to distinguish risk and trust behavior to a certain extent. This implies that the first transaction done by consumers with online companies will be “risky” behavior as opposed to “trusting” behavior since there will be no prior relationship.

In this paper, the focus is on initial trust or where the relationship does not exist between the online company and consumers. Consistent with TPB, in this study, risk and trust will be conceptualized as beliefs which will impact the intention to transact in e-commerce. Trust beliefs relate to the degree to which consumers believe that online companies are capable of conducting transactions and protecting consumer information. Risk perception or risk beliefs refer to the uncertainty that may be encountered in providing personal information to online companies.

1.3 Research Motivations

Current research in consumer behavior, privacy and e-commerce has examined the relationship of privacy, security and trust with behavior in separate studies. Trust and consumer behavior have been well researched in e-commerce research (Jarvenpaa et al. 2000; McKnight et al. 2002b; Pavlou 2003). Privacy and consumer behavior have been studied (Smith et al. 1996; Stewart and Segars 2002). Researchers have also studied security and consumer behavior (Salisbury et al. 2001; Suh and Han 2003). Adoption of e-commerce requires a consumer to make decisions in an environment of opposing forces (i.e. privacy and security concerns, risk perception and trust). Therefore, it is important to study the adoption of e-commerce in a holistic way by considering the impact of these related important factors. To author's knowledge, this is the first study to analyze these factors jointly in a single study. The main motivations of this study are: to provide a clear delineation of privacy and security concerns; to provide an integrative framework of e-commerce adoption by adapting privacy and security concerns, trust beliefs and risk perceptions; and empirically validate the proposed framework. In summation, this study is undertaken to answer the following research questions: 1) how do privacy and security concerns, and trust beliefs relate to attitudes of consumers? 2) What are the inter-relationships of privacy concerns, risk perception and trust beliefs and how do these factors affect consumer behavior intention to take part in e-commerce?

CHAPTER 2

REVIEW OF THE LITERATURE

The levels of analysis in privacy research identified by Greenaway and Chan (2005) are as follows: individual (consumer/employee), organizational, and sectoral/national. At the individual level, researchers have studied consumer attitudes about privacy (Culnan 1993; Sheehan and Hoy 2000). At the organizational level, important issues that have been studied are information privacy as it relates to organizational liability, decision outcome and ethical imperative (Greenaway and Chan 2005). At the sectoral/national level, issues regarding information privacy across industries and countries have been addressed (Earp et al. 2002). This study will address the privacy issues at the level of individuals.

2.1 Privacy Concerns and Actions for Privacy Protection

Privacy concerns or unwillingness to disclose personal information is seen as a major threat to e-commerce and the digital economy (Culnan 2000; Malhotra et al. 2004). Awareness of information collection and usage beyond the original transaction are the main influences on the degree to which consumers have privacy concerns (Sheehan and Hoy 2000). Smith et al. (1996) developed a measure to capture individuals' concerns about organizational

information privacy practices. Their measure was based on four dimensions: collection, unauthorized secondary use, improper access, and errors. This measure was later validated by Stewart and Segars (2002). Drawing upon the social contract theory, Malhotra et al (2004) developed the Internet consumers' information privacy concerns that consists of three dimensions – collection, control and awareness.

Actions that are taken to protect consumer privacy include industry self-regulation and procedural fairness (Culnan 2000; Culnan and Armstrong 1999). However, it is doubtful that such measures to maintain privacy have been successful. In answer to privacy concerns, consumers have resorted to using their own strategies to protect their privacy. A recent survey of online shoppers reported growing confidence in e-commerce (Saunders 2004). One reason given by consumers for their increasing confidence is that despite their privacy concerns, consumers are becoming smarter about their online habits.

2.2 Security Concerns

In addition to privacy concern, the security of consumer information has been recognized as one of the deterrents in the growth of e-commerce (Gray 1999). Rose et al. (1999) identified six categories of technological impediments inhibiting the growth of e-commerce: download delays, interface limitations, search problems, inadequate measures of web application success, security, and the lack of Internet standards. Although security concerns have a close relationship with privacy concerns, it is a different construct (Belanger et al.

2002; Vijayasarathy 2004). Consistent with the distinction made by Hoffman et al. (1999a), conceptualization of privacy and security concerns can be identified as different as ‘control over secondary use of information’ and ‘environmental control’ (Belanger et al. 2002). Environmental control refers to the ability of consumers to control the actions of other people in the environment during a market transaction or commercial exchange (Hoffman et al. 1999a).

In e-commerce, environmental control relates to the use of security controls that ensure the secure transmission of personal information during transactions (Belanger et al. 2002). E-commerce security is maintained through the use of technologies, such as encryption and authentication. Encryption of data involves using mathematical algorithm to scramble the message. The recipient of the message can read the message by descrambling the message using his decrypting key. Internet browsers have secure socket layer (SSL) technology that encrypts the message passed from the consumer to the online company. In addition to SSL, online companies also use secure electronic transaction (SET) which is an encryption technology that protects credit card information by allowing only the payment clearinghouse to access the credit information. SET is similar to SSL but the online company will not get access to credit card information.

Authentication involves the use of digital certificates and digital signatures to verify the identity of transacting parties (Hoffman et al. 1999b). A digital signature, comprised of uniquely identified bits, is issued by a trusted

third party known as the certificate authority (CA). It is an electronic signature that can be used to verify the identity of the message sender or the signer of a document. The use of digital signature helps to ensure that the original content of the message or the document has not been changed. A digital certificate is similar to an electronic version of a credit card that establishes consumer's credentials during an electronic transaction. It is also issued by CA. These technologies help to secure consumer information.

Environmental control strives to alleviate consumer concerns regarding personal information exchange with online companies due to fear or expectations of threats to online security from hackers or fear of identity theft (Belanger et al. 2002; Hoffman et al. 1999a). It is important to note that online companies also have their security concerns regarding the security of their consumer data. For the purpose of this paper, security concerns of the individuals only are considered, not that of the online companies.

The open architecture of the Internet makes it vulnerable to various security threats such as credit card information theft, personal information breaches, computer hacking, identity theft and infection of personal computers with viruses and spyware. These security threats fuel consumer concerns and have been noted as one of the major barriers for e-commerce (Udo 2001). Security concerns of consumers are defined as one's beliefs that online companies will not be able to safeguard the transaction information from security breaches during transmission and storage (Salisbury et al. 2001). In

this paper, security concerns refer to the extent to which one believes the personal information transmitted over the Internet would be secure and would not be accessed by unauthorized parties.

2.3 Risk Perceptions and Trust

Risk has been viewed as the uncertainty associated with the outcome of a decision (Sitkin and Pablo 1992). In e-commerce literature, two categories of risks are identified – product and transaction risks (Chang et al. 2005). Product risk refers to the uncertainty that the purchase will match the acceptance levels in buying goals or objectives. Transaction risk is the uncertainty that something unfavorable and unforeseen may result during the transaction process.

Transaction risks include authentication, privacy, security and non-repudiation of the transaction. Authentication risk refers to the uncertainty that the true identity of the seller is not revealed. Privacy risk refers to the possibility of theft of private information (Pavlou 2003). Security risk relates to the safety of the data transmitted over the Internet (Chang et al. 2005). Nonrepudiation refers to ensuring that a transferred message has been sent and received by the parties claiming to have sent and received the message (Suh and Han 2003). Nonrepudiation ascertains that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. Digital signatures are used to ensure nonrepudiation.

To mitigate risk perception, creating trust has been recognized as an important antidote (McKnight et al. 1998). Trust has generated a great deal of

research in organizational studies. The common theme of trust found across different disciplines can be defined as follows (Hosmer 1995):

- Trust is expressed as a form of optimistic expectation on the part of an individual regarding an outcome of an event or the behavior of another person;
- Trust normally occurs under conditions of vulnerability to the interests of the individual and dependence upon the behavior of other people;
- Trust is associated with willing, not forced, cooperation and with expected benefits resulting from that cooperation;
- Trust is difficult to enforce; and trust accompanies an assumption of accepted duty to protect the rights and interests of others.

Trust at the individual level is distinct from the trust at the group level (Zaheer et al. 1998). For instance, trusting a sales person would be different from trusting the company the sales person works for. Trust can be viewed as personality traits that are relatively stable intrinsic characteristics shaped by developmental and social factors extraneous to a given context (Webster and Martocchio 1992). Mayer et al. (1995) proposed a trust model with its antecedents and outcomes. They define trust as the “willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party”(Mayer et al. 1995). In this study,

trust is seen as the willingness of consumers to participate in e-commerce with belief that the companies will not misuse their personal information.

2.4 Intention to Transact in E-commerce

E-commerce in this study is broadly defined as the online exchange relationship between consumer and online companies, or web vendors. This study considers the intention to transact in e-commerce, which comprises purchasing a good or service from a web vendor, thus employing the Business to Consumer (B2C) model of e-commerce.

One of the important streams in IS research studies how and why individuals accept and adopt new information technologies (Agarwal and Karahanna 2000; Davis 1989a; Karahanna et al. 1999). At the individual level, usage of IT is studied by analyzing the role of intention as the predictor of behavior (Liu et al. 2004; Malhotra et al. 2004). Studies in this stream focus on determinants of intention such as attitudes, social influences and contexts. These studies are grounded in models of social psychology such as, the theory of reasoned action (TRA) (Ajzen and Fishbein 1980) and the Theory of Planned Behavior (TPB) (Ajzen 1985; Ajzen 1991). Intention, as the determinant of behavior has been well-established in IS and other reference disciplines (Ajzen 1991; Taylor and Todd 1995). According to the TRA, intention predicts behavior. Intention is formed by subjective norm and attitudes, which in turn is shaped by beliefs. A TRA based model is suitable to predict the behavior of activities which are under volitional control. Volitional control means that the

user is fully able to control the performance of an activity. In case of non-volitional control activities, the TPB is better suited since it has the additional component of perceived behavioral control (PBC) as the determinant of intention. The Technology Acceptance Model (TAM) which is an adaptation of the Theory of Reasoned Action (TRA) has been popular with IS researchers to determine the antecedents of system usage through beliefs about two factors: the perceived ease of use, and the perceived usefulness of an information system (Davis 1989b). Earlier studies of adoption of E-commerce have widely used the TAM (Gefen et al. 2003; Liu et al. 2004; Vijayasarathy 2004) and TRA (Jarvenpaa et al. 1999; Malhotra et al. 2004; McKnight et al. 2002b; Pavlou 2003).

The TPB is preferred over the TAM in this study because privacy and security concerns are the first hurdle that consumers have to cross in order to decide to take part in e-commerce before being influenced by the usability features of a website. As shown by Yang and Jun (2002), security was the key concern for a consumer who choose not to buy online. Another study found that perceived security was a much stronger determinant of intention to purchase online than the perceived ease of use and usefulness of the website (Salisbury et al. 2001). Privacy and security concerns are the primary reason consumers are not purchasing over the web (Udo 2001). The potential threats to consumers who use credit cards to purchase over the web have been well covered by the media. However, online companies also face a major threat of

payment frauds. Therefore, security concerns perceived by both consumer and online company remain as barriers to e-commerce. As for the scope of this study, the security concerns of consumers only are considered.

2.5 The Theory of Planned Behavior

In this study, the Theory of Planned Behavior (TPB) as proposed by Ajzen (Ajzen 1985; 1991) will be adopted. In e-commerce, online consumers face new constraints such as the impersonal nature of the online environment, extensive use of IT, and the uncertainty of the open infrastructure, thus supporting the use of perceived behavioral control (PBC) in the adoption model (Pavlou and Fygenson 2006). When a consumer intends to participate in e-commerce, his/her intentions are shaped by the attitudes formed regarding the online company. Attitudes are shaped by salient beliefs. In addition to attitudes, the feeling of what others would feel about taking part in e-commerce and one's control over the process of taking part in e-commerce also determine the behavioral intention.

According to the Theory of Reasoned Action (TRA) (Ajzen and Fishbein 1980), intention is the determinant of behavior. Intention, in turn, is determined by attitude and subjective norm. In the conceptual framework put forward by Fishbein and Ajzen (1975), beliefs about an object forms the basis for the formation of attitude toward the object. Therefore, attitudes are usually measured by assessing a person's beliefs. Assessing a person's beliefs and its formation process is an integral part to assessing the change of attitudes and

intentions. Fishbein and Ajzen (1975) define beliefs as “the subjective probability of a relation between the object of the belief and some other object, value, concept or attribute.”

In the context of e-commerce, this implies that when a consumer visits an online company, he may perceive that the online company has some attribute of trustworthiness. Indirect factors related to the trustworthiness of an online company may be reputation, popularity and recommendation of others to participate. The direct observation by the consumer of such attributes includes noticing third-party trust seals on websites. Such direct observations of the online company result in the formation of *descriptive beliefs* (Ajzen and Fishbein 1980) of the online company. Beliefs are also formed in ways other than by direct observations. Interaction with an online company may change or form new beliefs of a consumer. If a consumer has experience in buying on the Internet and he has found it to be a satisfactory experience, he may likely have positive beliefs towards online companies. Likewise, if the consumer also has the experience of buying from the online company in an offline setting then he may be more likely to have positive beliefs (Chellappa 2005). Beliefs that go beyond directly observable events are known as *inferential beliefs* (Ajzen and Fishbein 1980). In addition to descriptive and inferential, beliefs can be formed by getting information from other sources such as media, books, magazines, online companies, search engines, friends, colleagues, or family members. Such beliefs are known as *informational beliefs* (Ajzen and Fishbein 1980).

The attitude of an individual with respect to some object, action, or event may be positive or negative. It is a subjective evaluation that an individual forms. According to Fishbein and Ajzen (1975), an attitude represents “a person’s general feeling of favorableness or unfavorableness towards some stimulus object.” A belief such as risk or trust towards an online company vendor is a function of the individual’s evaluations of the attributes of the online company. Individuals have their own attribute evaluations when they face new objects which depend upon the association of the new objects with other objects, attributes, or qualities towards which we already have attitudes. For example, a consumer will evaluate the characteristics, such as security features of an online company, based on what he has been exposed to in other online companies and past experiences of online buying and Internet experience.

A larger number of beliefs are responsible for forming the attitude of a person towards an object. However, all the beliefs do not have the same amount of effect on the attitude. Only a relatively small number of beliefs appear to be the determinants of a person’s attitude at a given moment. Such beliefs are known as salient beliefs. A belief that is salient at a given moment may not be salient at another point in time. Salient beliefs are likely to change and get replaced by new beliefs. The expectancy-value model can explain the relation between a set of beliefs and attitude (Fishbein 1967). The underlying assumption in the expectancy-value model is that people are goal-oriented, and their behaviors are performed in response to their beliefs and values with an

objective to achieve a goal. According to the expectancy-value model, behavior is a function of the expectancies a person has, and the value of the expected goal toward which that person is working. The way a person evaluates an attribute adds to his attitude and is shaped by the strength of his beliefs. According to the expectancy-value model (Fishbein 1967), attitude can be estimated by multiplying the evaluation of each attribute associated with the object by the subjective probability that the object possesses that attribute and finally aggregating the products for the total set of beliefs. Therefore, people holding the same beliefs may have different attitudes, and people holding different beliefs may have the same attitudes (Ajzen and Fishbein 1980). For example, consumers holding high trust beliefs may have varied attitude towards an online company which may be subjected to different levels of risk they perceive with that company. The theory of planned behavior is shown in Figure 1.

In this study, antecedents of attitude are added to extend the TPB. These antecedents (i.e. risk perception and trust beliefs) will shape the attitude of consumers and determine their intention whether or not to take part in e-commerce. Drawing upon social contract theory, Malhotra et al (2004) developed a scale to measure the dimensions of privacy concerns of the Internet users and presented a causal model to describe the influences of privacy concerns on a consumer's decision to release personally identifiable

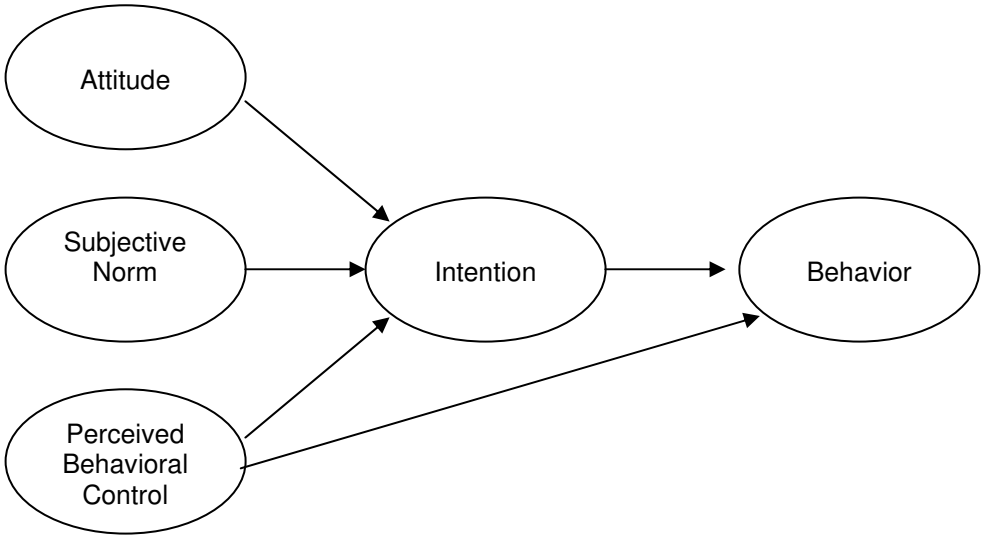

Figure 1. The Theory of Planned Behavior (Ajzen 1991)

information in a certain situation. This study builds upon the causal model developed by Malhotra et al. (2004) by including other factors such as, the security concerns of consumers, attitudes, subjective norm and perceived behavioral control. A distinction of this study with Malhotra et al (2004) is that the phenomenon of interest is the intention to transact in e-commerce, mainly purchasing from online companies, rather than just giving out personal information to obtain membership from websites. The model developed by Malhotra et al (2004) is presented in Figure 2.

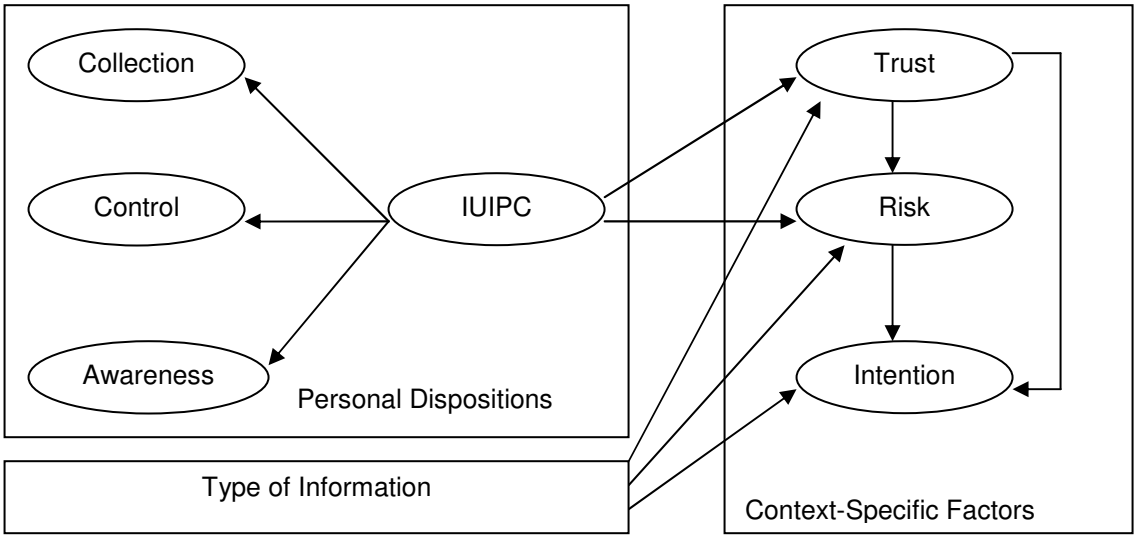

Figure 2. A model of consequences of IUIPC (Malhotra et. al 2004)

CHAPTER 3

MODEL AND HYPOTHESES

In this section, a model is developed to study how consumers' concerns about privacy and security, and trust beliefs affect their intention to engage in e-commerce transactions. The proposed model, as shown in Figure 3, builds upon existing models of e-commerce adoption. The theoretical framework of trust and risk (Jarvenpaa et al. 1999; Mayer et al. 1995) and the Theory of Planned Behavior (Ajzen 1991) are used as the background for the proposed model.

3.1 Trust Beliefs

Most recently, e-commerce researchers have started to study trust in online contexts (Gefen et al. 2003; McKnight et al. 2002a; Pavlou 2002). Trust has been studied extensively in organizational studies (Kim and Mauborgne 1993; McAllister 1995; Roberts and O'Reilly 1974). Mayer et al. (1995) proposed an integrative definition of trust as "the willingness of a trustor party to be vulnerable to the actions of trustee party based on the expectation that the trustee party will perform a particular action important to the trustor party, irrespective of the ability to monitor or control the trustee party." In e-commerce, consumers are the trustor party while online companies are trustee parties. Consumers are vulnerable to the actions of online companies since the

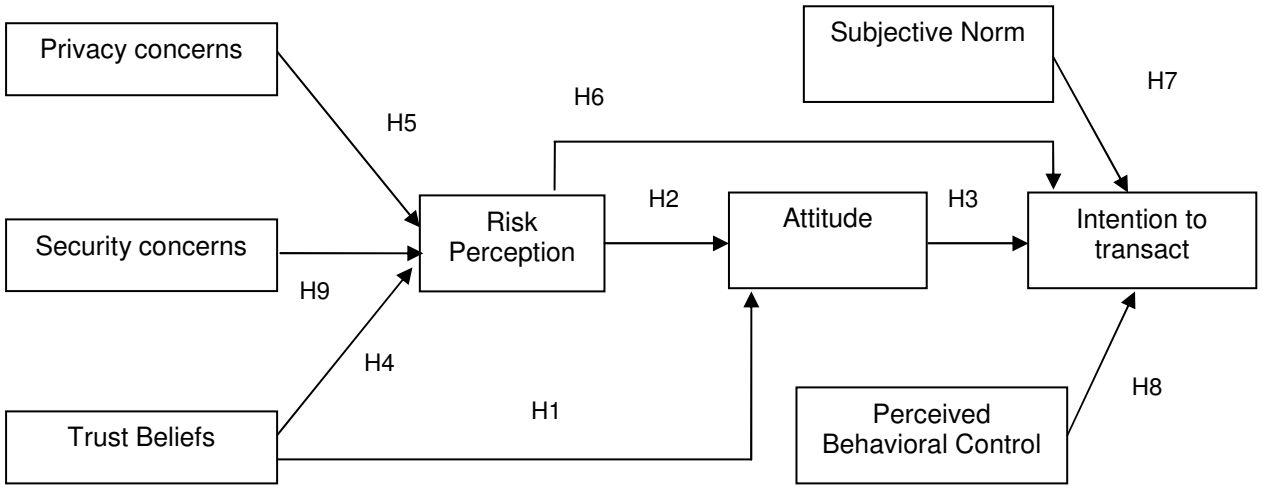

Figure 3. The Research Model

provide sensitive information such as credit card information, addresses and emails when they intend to participate in electronic transactions. Consumers have only limited ability to monitor the actions of the online companies regarding the unauthorized use of personal information; hence, there is an inherent unwillingness on the part of consumers to share their personal information. Therefore, trust is needed to relieve the concerns of consumers (Luo 2002).

In literature, trust has been conceptualized variously as a belief, attitude, intention and behavior (Mayer et al. 1995; McKnight et al. 1998). Being a psychological state, trust is clearly distinct from behavior; rather it is an antecedent to the behavior (Bhattacherjee 2002). In this paper, trust is conceptualized as beliefs. The dimensions of trust beliefs described by Bhattacherjee (2002) are ability, integrity and benevolence. Ability refers to the consumer's perception of online company's competencies and knowledge salient to the expected behavior. These perceptions may result from prior experience or institutional endorsements from third parties in forms of trust seals. Integrity refers to the consumers' perception that the online company will adhere to a set of principles or rules of exchange acceptable to the consumer during and after the exchange. Benevolence is the extent to which an online company is perceived to be acting for the well-being of consumer.

In an e-commerce scenario, a user's beliefs about an online company may be captured by trust and risk perception. Attitude may be either favorable

or unfavorable. A favorable attitude will form the intention to take part in an e-commerce transaction. Intention is then followed by the actual behavior of buying from the online company. Trust beliefs are formed by consumers based on the information available about the companies. Trust in an online company can generate a favorable attitude in a consumer and may also improve the attitude indirectly by lowering the risk perception of the consumer (Jarvenpaa et al. 1999). Thus, the hypothesis to be tested is:

H1: Trust beliefs positively influence consumer attitudes towards online companies.

3.2 Risk Perception and Attitude

Risk perception was first conceptualized by Bauer (1967) in marketing literature as consumer behavior in the theoretical framework of risk taking. According to the risk taking framework, consumers decide to buy a product under some degree of uncertainty about a given brand. Assuming perceived risk, consumers take steps to reduce it, mostly by relying upon a person or idea (Sheth and Venkatesan 1968). For instance, a consumer may rely on the brand image of a product or on the opinion of an expert. Risk perception is used as a surrogate of risk since it is difficult to capture risk as an objective reality. Risk perception is defined as the subjective probability of suffering a loss in pursuit of a desired outcome.

Sitkin and Pablo (1992) suggested that perceived risk may mediate the effect of trust on intention and behavior. Few studies have investigated the

effect of trust on perceived risk. A significant negative effect between trust and perceived risk was found (Jarvenpaa et al. 1999; Jarvenpaa et al. 2000; Kimery and McCord 2002; van der Heijden 2003). Data collected from an online auction marketplace indicated that buyers' trust in sellers facilitated online transactions by reducing perceived risk (Pavlou and Gefen 2004). In this study the following hypotheses will be addressed:

H2: Risk perception negatively influences consumer attitudes towards online companies.

H3: Favorable attitudes towards online companies will increase the consumer's intention to purchase.

As pointed out by Malhotra et al. (2004), it has been established in the trust-risk literature that personal traits influence trust and risk beliefs (Mayer et al. 1995; McKnight et al. 1998). If a consumer is too concerned about privacy it will influence how she will trust an online vendor, or perceive risk in purchasing from the vendor. In the context of e-commerce, a negative relationship between privacy concerns and trust, a positive relationship between privacy concerns and risk, and a negative relationship between trust and risk is shown (Malhotra et al. 2004). It is suggested in the literature that privacy protection may be an important antecedent in building trust. Online companies can build trust if they convince the consumer that online transactions will take place as expected by the consumer (Culnan and Armstrong 1999). Liu et al. (2004) proposed that the

trustworthiness of an online company may depend on the beliefs of consumers that their privacy is maintained. Thus, the following hypotheses will be tested:

H4: A high level of trust beliefs will reduce risk perception.

H5: A high level of privacy concerns will increase risk perception.

Although a favorable attitude may influence consumers to take part in e-commerce, the level of risk perception plays a strong deterrent. The risk perception associated with online shopping may reduce the consumer's perception of control and thus, may negatively influence the willingness to buy online (Jarvenpaa et al. 2000). Risk perception was found to be significant with consumer's willingness to buy books from websites (Jarvenpaa et al. 2000). Therefore, the next hypothesis is as follows:

H6: A high level of risk perception will lower the intention to transact in e-commerce.

3.3 Behavioral Intention

Behavioral intention is an antecedent to actual behavior (Ajzen 1991). The TPB suggests that behavioral intention is the most influential predictor of behavior. The components of the proposed research model are shown in Figure 3. Because of difficulties in measuring actual behavior in a field survey where the measures are self-reported, this study will only measure behavioral intention only. With self-reports it is hard to determine whether the behavior actually took place even though the respondents reported their behavior. In the absence of an objective measure for behavior, measuring intention appears reasonable.

Prior literature exist where behavioral intentions were measured instead of actual behavior (Malhotra et al. 2004; McKnight et al. 2002b; Smith et al. 1996; Stewart and Segars 2002). There is evidence in prior studies that shows that behavioral intention correlates with actual behavior (Sheppard et al. 1988; Venkatesh et al. 2003). Therefore, measuring intention will give some indication of consumer behavior.

3.4 Subjective Norm

In the TPB, one's subjective norm towards a behavior is defined as one's assessment of whether or not people important to him/her feel the behavior should be performed (Ajzen 1991). This assessment is conducted for a number of relevant referents such as, friends, family and co-workers. The belief based measurement of subject norm consists of normative beliefs and motivation to comply. Normative beliefs refer to assessment of how likely or unlikely the referent groups support the behavior. Motivation to comply refers to personal assessment of how motivated one is to comply with referent groups. The TPB suggests a positive relationship between subjective norm and behavioral intention. This has been shown in the empirical work of intention to use on-line shopping (Vijayasarathy 2004). For this study, subjective norm refers to the degree that a consumer's referent group approves the e-commerce adoption. Only normative beliefs are considered in this study since motivation to comply is more suited for organizational studies where individual's referent groups will be co-workers. The hypothesis to be tested follows:

H7: Subjective norms of consumer have a positive relationship with intention to purchase from online companies.

3.5 Perceived Behavioral Control

Perceived behavioral control (PBC) is posited to have a positive relationship between intention and actual behavior. According to Ajzen (1991), PBC relates to how easy or difficult it would be to carry out a certain behavior. PBC denotes a subjective degree of control over the performance of a behavior rather than the perceived likelihood that a behavior will result in a certain outcome (Ajzen 2002). For this study, perceived behavioral control is defined as a consumer's perceived ease or difficulty in buying from the online company.

H8: Perceived behavioral control positively influence intention to purchase from online companies.

3.6 Security Concern

There has been a limited research which has studied the relationship amongst security, risk perception and purchase intention. In most cases, security has been included as a part of privacy concerns. This practice is also evident in the concern for information privacy (CFIP) instrument developed by Smith et al. (1996). The four dimensions in CFIP were collection, errors, unauthorized secondary use and improper access. Of the four dimensions, improper access appears similar to what Hoffman et al. (1999a) referred to as environmental control, which is closely related to security concerns.

Among the very limited empirical studies on security, Miyazaki and Fernandez (2001) found that system security concerns of the consumers were related to the rate of online product purchasing. However, no negative correlation between the presence of privacy and security statements and the perceived risk was found (Miyazaki and Fernandez 2000). In the same study, privacy and security statements were positively related to online purchase likelihood. Testing the role of risk perception in the relationship between privacy and security concerns and the purchasing intention, Miyazaki and Fernandez (2001) found some support for its mediating role. This empirical evidence is in contrast with the results of another study by Harris Interactive (2001). They found that only 25% of consumers seem to recognize privacy and security seal features on web sites. In light of mixed empirical evidence of the limited research on security, it is necessary to test the following hypothesis:

H9: A higher level of security concern increases risk perception.

CHAPTER 4

OPERATIONALIZATION OF RESEARCH VARIABLES

This study used a survey instrument to collect data on the variables in the conceptual model illustrated in Figure 3. Table 1 lists the procedure to be followed for instrument development as suggested by Churchill (1979). The next subsection gives an overview of the field study. The following sections outline the definitions of the variables and the reference literature that are the sources for the adapted instruments into the design of the survey instrument.

Table 1. Procedure for developing measures

Item Generation	Step 1: Specify domain Step 2: Generate sample of items
Item Refinement	Step 3: Pretest Step 4: Pilot test
Confirmatory Analysis	Step 5: Collect data Step 6: Assess reliability Step 7: Assess validity Step 8: Initial Confirmatory Factor Analysis on initial measurement model Step 9: Final Confirmatory Factor Analysis

4.1 Measures

The survey asked participants to choose an online company they are familiar with and assume that they are interested in buying a product offered by that company. They were asked to complete the questionnaire survey keeping in mind their chosen online company. A seven-point Likert scale ranging from strongly disagree (1) to strongly agree (7) was used for the responses. The sources of the scales, shown in Table 2, are discussed in the following section. Item measures are included in Appendix A.

Privacy concerns

Privacy concerns of an individual in the context of e-commerce are influenced by external conditions (i.e. industry sectors, cultures, regulatory laws) as well as individual's perceptions of those external conditions. A ten-item Likert type scale was adapted from Malhotra et al. (2004). The privacy concern measure is used as a second order construct with three underlying dimensions of collection, control and awareness. The number of items for the three dimensions was 4, 3 and 3 respectively.

Table 2. Item map			
Constructs	**Variables**	**No. of Items**	**Related literature**
Privacy Concern	Collection	4	Smith et al. (1996)
	Awareness of Privacy Practices	3	Malhotra et al. (2004)
	Control	3	
Security Concern	Perceived web security concern	3 2	Salisbury et al (2001) Newly developed
Risk Perception	Riskiness, potential for loss, and safety	3	Malhotra et al. (2004)
Attitude	Attitude of individual	2	Pavlou and Fygenson (2006)
Perceived Behavioral Control	The level of difficulty	1	Pavlou and Fygenson (2006)
Subjective Norm	Normative beliefs	2	Pavlou and Fygenson (2006)
Trust	Trust Beliefs	8	Bhattacherjee (2002)
Gender	Gender	1	Smith et al. (1996)
Age	Age	1	Smith et al. (1996)
Internet Experience	Internet Experience	1	Smith et al. (1996)
Falsify ID	Provide misinformation	1	Smith et al. (1996)
Privacy Victim	Invasion of privacy in past	1	Smith et al. (1996)
Media Exposure	Media exposure	1	Smith et al. (1996)
Education	Education	1	Smith et al. (1996)

Total Items: 38

Security concerns

Security concerns refer to the extent to which one believes the personal information transmitted over the Internet would be secure and would not be accessed by unauthorized parties. A three-item Likert type scale is adapted from Salisbury et al. (2001). Two items were newly developed. These items are sec4 and sec5 as shown in Appendix A.

Trust beliefs

The scale measuring trust beliefs is adapted from Bhattacherjee (2002). The dimensions of trust were ability, benevolence and integrity. An eight- item likert type scale including one that measured the overall trust was adopted.

Risk perception

Risk perception refers to the uncertainty the consumers feel while deciding to purchase from online companies. Risk perception measures were based on Jarvenpaa et al (1999) and Malhotra et al. (2000; 2004). Three-item likert scale was adapted.

Attitude

Attitude has been operationalized as the consumer's evaluation of the desirability of using an online company to buy a product. Attitude is measured by two-item likert scale from Pavlou and Fygenson (2005).

Subjective norm

Subjective norm refers to the consumer perceptions of whether a certain behavior is accepted by one's referent group. Two-item likert scale to measure subjective norm was adapted from Pavlou and Fygenson (2005).

Perceived behavioral control

Perceived behavioral control is defined as the perception of an individual regarding the difficultness to carry out a certain behavior. A single-item likert scale was adapted from Pavlou and Fygenson (2005).

Behavioral intention

Behavioral intention in this study is the consumer's willingness to purchase from an online company. Behavioral intention to purchase was adapted from Malhotra et al (2004). It was measured by two-item likert scale.

4.2 Survey Administration

4.2.1 Pilot Study and Pretest

A pilot study was carried out to validate the instrument developed for this study. The pilot study served several purposes: 1) to determine the time taken for filling out the survey to ensure that the length of the instrument was reasonable, 2) to test the reliability and validity of the context and the instrument, 3) refinement of the instrument. The confidentiality of respondents for the pilot test was ensured. After the pilot test, some modifications were done to the instrument to improve the clarity. For example, on one of the items regarding security concern, the original wording of "I am hesitating to make

purchases from the Web because I am concerned about security issues of sensitive information" was changed to "I hesitate to make purchases from the Web because of security issues of sensitive information." The pilot study was conducted with a group of 34 undergraduate business students. The respondents were 52.9% male and 47.1% female. The age distribution was as follows: 26.5% were from 17 to 20 years old; 50% were 21-29; 11.8% were 30-39; 8.8% were 40-49 and 2.9% were above 49 years. Time taken for completing the survey was determined to be approximately 20 minutes. This being a reasonable length of time, no action was taken to shorten the instrument.

Although the measures were adopted from the literature it was necessary to conduct the validity and reliability tests since they are used in a different context in this study. Content validity refers to whether the questionnaire items or measures are representative of the ways that could be used to measure the content of a given construct (Kerlinger 1964). As suggested in Straub (1989), content validity is established through literature reviews and expert judges or panels. A literature survey was done to find all possible relevant measures. A pretest study was done with three IS faculty members and two doctoral students. The participants were asked to review and evaluate the instrument. Based on the suggestions, minor revisions were made to the instrument to clarify questions. For example, the use of words such as "Internet" and "Web" to mention the World Wide Web was revised and

changed to “Web” across the instrument. The “web vendor” was also changed to “online company” to bring consistency throughout the instrument.

Construct validity was established by demonstrating that the reasonable operationalization of the construct is done. The constructs being validated are related to other constructs as suggested by the theory. Further, the constructs do not correlate with other theoretically unrelated constructs and variables. Principal Component Analysis with Varimax rotation was used to determine if all the items hang together and load onto related factors. Factors with eigen values greater than 1.0 were retained. All the scales except for the privacy concerns scale loaded onto one factor. Privacy concerns loaded onto three factors as expected since this instrument was adapted from Malhotra et al. (2004), which had three factors of control, awareness of privacy practices and collection. Factor loadings for privacy concern scale are shown in Table 3.

Table 3. Factor Loadings for Privacy Concerns

	Component		
	1	2	3
CON1	.053	**.940**	.134
CON2	.438	**.811**	.024
CON3	.383	**.693**	.280
PAW1	**.924**	.115	.129
PAW2	**.930**	.234	.058
PAW3	**.873**	.176	-.069
COL1	.158	.092	**.949**
COL2	.469	.176	**.724**
COL3	.358	.129	**.822**
COL4	.248	.222	**.745**

Reliability of the multi-item scales was tested with Cronbach's alpha. All the multi-item scales met the cut-off criteria of 0.70 as suggested by Nunnally (1978). Table 4 shows the results of the reliability tests.

Table 4. Reliability of the Constructs

Construct	Number of Items	Cronbach's α
Control	3	.741
Awareness	3	.772
Collection	4	.874
Security Concern	5	.844
Trust Beliefs	7	.832
Risk Perception	4	.854
Attitude	2	.902
Subjective Norm	2	.820
Intention	2	.902

4.2.2 Power Analysis

In order to determine that the study will have a reasonable probability of detecting a significant finding, power analysis was conducted. Statistical power refers to the probability that statistical significance will be indicated when it is present (Hair et al. 2002). Power depends on the effect size, significance criterion (α) and sample size. Effect size represents the magnitude or strength of the relationship among the variables in the population. The larger the effect size the greater the probability that it will be detected and the null hypothesis is rejected. The significance criterion is the chosen risk of committing Type I error. The larger the α, the higher is the power. Sample size is likely to influence the precision of sample estimates. The larger sample size increases the power by minimizing the error variance and by influencing the precision (Hair et al. 2002).

Assigning a high level of power such as .80 gives the research study a sufficient probability of finding a true effect (Baroudi and Orlikowski 1989). For this study, α is set at 0.05, power is set at .80 and the effect size as medium. Based on the power tables provided by Cohen (1992), the suggested sample size for eight predictors would be at least 107.

The sample size requirements for the Partial Least Squares (PLS) Regression approach is much less than that required for covariance-based structural equation modeling (SEM). According to Chin (1998), sample size requirements for PLS can be determined in the following ways: 1) the construct with the largest number of formative indicators or 2) the dependent latent

variable with the largest number of relationships. The sample size required will be 5 to 10 times of either 1) or 2) whichever is higher. Since there were no formative indicators in this study, the latent variable with the most number of relationships was “intention” with four predictors and seven control variables. Following Chin (1998) the sample size required would be around 110. However, Goodhue et al. (2006) forewarns that “10 times” rule for sample size should not be used as a guideline while using either PLS or regression for anything except for a strong effect size with high reliability. Therefore, it was determined that adequate sample size over 200 would be needed to ensure sufficient power for the data analysis.

4.2.3 Actual Study

Data were collected from 273 undergraduate business students. The motivation to participate in the survey was a chance to be included in a drawing for a $50 gift card. The respondents were assured for full confidentiality of their responses. It was completely voluntary for students to participate in the draw. Those who wanted to be included in the draw provided a valid email address for notification if they win. A total of 124 students participated in the draw.

In the main survey as well as the pilot study, the respondents were asked to select a specific product that they plan to purchase in the next six months. After selecting a product, the respondents were asked to report an online company that they have recently visited which offers the selected product. The respondents were asked to fill out the survey with regard to their

selected online company. Time given was approximately 20 minutes since it was determined from the pilot study as the normal required time for completing the survey.

4.2.4 Demographics of the Sample

The age distribution was as follows: 29.4% were from 17 to 20 years old; 44.5% were 21-29; 13.5% were 30-39; 9.2% were 40-49 and 3.4% were above 49 years. Out of 273 respondents, 138 were male and 131 were female. 4 respondents did not mark the gender item. 57.5% were full-time students while 42.5% were part-time students. Table 5 shows the sample characteristics.

Table 5. Characteristics of the Sample

	Mean	**Standard deviation**	**Missing**
Age	25.5	6.45	2
Internet Experience	6.88	1.52	0
Gender	Male Female	138 131	4
Note: Age and Internet Experience are given in number of years.			

CHAPTER 5

ANALYSIS AND RESULTS

The main objective of this research was to determine whether or not the aforementioned antecedent variables are significant predictors of behavioral intention to take part in e-commerce. Therefore, it is essential to choose a data analytical approach that is most appropriate for the given study. The chosen statistical technique should help to ensure that results portray the phenomenon of interest as closely as possible, which, in this case, is the intention to transact in e-commerce. This chapter provides a brief explanation of the chosen statistical technique. This is followed by data analysis and results of the study.

5.1 Analytical Approach

As noted in Gefen et al.(2000), there are two possible approaches for analyzing the data for this study – first generation and second generation statistical approaches. First generation approaches have limitations to analyze data while more than one layer of relationships exists in the model. For example, in situations where there are two mediating variables in sequence between a predictor and criterion variable, first generation approaches can not simultaneously analyze the relationship. Rather, they have to break it into multiple analyses, each considering one layer at a time. Another limitation of

first generation approaches is that all measurement is made with error and the measurement error is generally lumped into a residual error term (Barclay et al. 1995).

Another approach is to use second generation statistical tools or structural equation modeling (SEM) techniques, such as partial least squares or PLS (Wold 1982) and covariance based approaches. One of the popularly used covariance based approaches is LISREL (Joreskog and Sorbom 1986). SEM permits the simultaneous analysis of multiple criterions and predictor constructs, the analysis of unobservable latent constructs and supports the application in a confirmatory mode. Unlike first generation techniques, SEM not only assesses the structural model (i.e. relationships among a set of independent and dependent constructs) but also the measurement model (i.e. loadings of observed items onto their latent variables) simultaneously in the same analysis (Gefen et al. 2000). The two most widely used software tools for SEM in the IS field are LISREL and PLS (Gefen et al. 2000).

PLS, a latent structural equation modeling technique, uses a component-based approach to estimation, thereby placing a minimal demand on sample size and residual distributions (Fornell and Bookstein 1982; Lohmoller 1989). PLS was preferred over LISREL in this study for several reasons: predictive accuracy, explanation of complex relationships, small sample size requirements, and lack of need for the assumption of multivariate normality. For

analyzing complex relationships and for prediction, PLS is a preferred method although LISREL also has the capability (Sambamurthy and Chin 1994).

Data was found to be non-normal after the inspection of histograms and scatter plots. Table 6 displays the descriptive statistics and the results of the tests for normality. Multivariate normality is not a requirement for estimating PLS parameters (Barclay et al. 1995). With LISREL, departures from normality require a much larger sample size, i.e. 15 respondents for each parameter. For this study with 19 parameters, the total sample size requirement would be 285. Covariance-based SEM software tools, such as LISREL, EQS and AMOS, tests the a priori specified model against population estimates derived from the sample and their main objective is theory testing (Gefen et al. 2000). On the other hand, PLS is designed to explain variance, i.e. to examine the significance of the relationships and their resulting r^2 or sample coefficient of determination, as in the case of linear regression. PLS is used both for predictive applications and theory building (Chin 1998). PLS was selected for this study since the emphasis was on theory building by extending on the theory of planned behavior, and also because of the sample size requirements. Furthermore, the PLS has also been widely used in IS research (Agarwal and Karahanna 2000; Gopal et al. 1992; Wasko and Faraj 2005).

PLS Graph version 3.0 was used for data analysis and testing the hypotheses presented in chapter 3. In PLS, estimation is based on ordinary least squares (OLS) fixed point iterations on subsets of model parameters, thus

requiring few distributional assumptions (Chin 1998; Fornell and Larcker 1981). The PLS algorithm consists of an iterative procedure that involves outer and inner models. The outer model represents a weighted aggregate of its own indicators. The inner model refers to weighted aggregate of other component scores that are related to the construct in the theoretical model. During each iteration, the inner model estimates are used to obtain the outside approximation weights while outer model estimates are used to obtain the inside approximation weights. In the first PLS iteration, an initial outer value is formed by simply summing the loadings. Then, the regression weights are estimated and these estimates are used as weights in a linear combination to give an inner value. This value is used in simple regressions to estimate new loadings. The next step uses the estimated loadings, transformed into weights, to form a new linear combination (Barclay et al. 1995). The iterative procedure ends when the percentage change of each outside approximation weight relative to the previous round is less than .001 (Chin 1998).

Having decided on using PLS, the data were analyzed using measured and structured model as described by Hulland (1999). The following sections provide discussion on data analysis.

Table 6. Descriptive Statistics and Tests for Normality						
			Skewedness		Kurtosis	
Construct	Mean	Std. Deviation	Statistic	Z-score	Statistic	Z-score
Control	5.669	1.130	-1.323	**-8.939**	2.969	**10.069**
Awareness	6.187	1.009	-1.990	**-13.445**	5.386	**18.263**
Collection	5.833	1.123	-1.663	**-11.279**	3.665	**12.473**
Security Concern	4.550	1.348	-0.349	**-2.368**	-0.290	-0.988
Trust	5.501	0.946	-0.662	**-4.467**	1.002	**3.392**
Risk	3.178	1.306	0.373	**2.524**	-0.452	-1.531
Attitude	5.733	1.304	-1.045	**-7.084**	0.755	**2.570**
PBC	5.835	1.265	-1.309	**-8.879**	1.673	**5.694**
Subjective Norm	5.399	1.213	-0.766	**-5.194**	0.335	1.139
Intention	5.815	1.435	-1.656	**-11.230**	2.704	**9.204**

Notes:

Z-scores in bold denote a significant departure from normality for skewedness and kurtosis (at $p < .025$).

All constructs except for Attitude, Perceived Behavioral Control (PBC) and Intention are seven-point scales with the anchors 1 = Strongly disagree, 4 = Neutral, 7 = Strongly Agree.

Attitude is a 7-point scale with two different anchors 1 = Very bad idea, 7 = Very good idea and 1 = Very undesirable, 7 = Very desirable.

Intention is a 7-point scale with anchors 1 = Unlikely, 7 = Likely.

5.2 Measurement Model

PLS estimates parameters for both the links between measures and constructs (i.e. loadings) and links between different constructs (i.e. path coefficients) simultaneously. However, the PLS model is usually analyzed and interpreted sequentially in two stages (Hulland 1999): 1) the assessment of the reliability and validity of the measurement model and 2) the assessment of the structural model. Following this sequence ensures that the instrument has

adequate reliability and validity before attempting to draw conclusions about the nature of the construct relationships.

The measurement model is assessed by examining in three ways as suggested by (Barclay et al. 1995): 1) individual item reliability, 2) internal consistency, and 3) validity between constructs .

5.1.1 Item Reliability

Individual item reliability, in PLS, is assessed by examining the loadings, or simple correlations, of the measures with the corresponding construct. Carmines and Zeller (1979) prescribe to accept items with loadings of .707 or more since it implies more shared variance between the construct and its measures than error variance. Table 7 indicates the loadings of the items on the constructs. Interpreting the loadings, twenty-nine out of the thirty-three items reach the .707 level of acceptable reliability. Some items did not reach the required level. This is common when standard or newly developed scales are used in causal modeling. Sometimes, scale items do not display the same psychometric properties when they are used in different theoretical and research contexts from the ones they were first developed in (Barclay et al. 1995). Three potential reasons may lead to low loadings of the items: 1) the item may be unreliable, 2) method bias – where the items share more in common with a method of measuring items rather than with the construct being measured, and 3) the item is related to a multidimensional construct. There are two options to deal with issues of low loadings: 1) carefully remove items such

that the original construct remains in the model, 2) consider modeling a construct into multiple dimensions by creating a higher order construct (Sambamurthy and Chin 1994). In the final study, the eighth measure of trust, TRU8, with loading of .3504 was dropped. Meeting the criteria of the first option, dropping the measure TRU8 still leaves the original construct of Trust in the model. The latent construct of trust was captured with the remaining seven items. As shown in Table 7, items on other scales reached the sufficient criteria of reliability.

5.1.2 Internal Consistency

Internal consistency refers to the degree to which the group of items used to assess a construct reflect a true, common score for the construct (Bagozzi 1980). The measure of internal consistency developed by Fornell and Larcker (1981) is used as a measure of reliability. In this study, internal consistency was determined by calculating two measures: 1) composite reliability (CR) of scales, 2) Average variance extracted (AVE) by the construct. Composite reliability examines the ratio of non-random variance associated with all measures of a construct to total variance associated with these measures using the following calculation:

$$\rho_c = \frac{(\sum \lambda_i)^2}{(\sum \lambda_i)^2 + \sum_i \mathrm{var}(e_i)}$$

where λ_i is the component loading to an indicator and $\mathrm{var}(e_i) = 1 - \lambda_i^2$ (Werts et al. 1974). The measure of composite reliability is not influenced by the number of items in the scale. This measure is similar to Cronbach's alpha as a measure of internal consistency except that Cronbach's measure presumes, a priori, tau-equivalency, or that each indicator of a construct contributes equally. However, the interpretation of the values is similar and the guidelines of 0.70 offered by Nunnally (1978) can be used. Table 8 displays the cronbach's alpha and composite reliabilities for the scales. Both the alpha and CR values for all the scales, ranging from .791 to .952 are above 0.70 which support their reliability.

AVE measures the amount of variance in a construct accounted by its indicators relative to measurement error (Fornell and Larcker 1981). The threshold for AVE is 0.50, signifying that 50 percent or more variance of the indicators has been accounted for by the construct (Fornell and Larcker 1981). If the AVE is less than 0.50 then the validity of the indicators and the construct may be questionable since the variance due to measurement error would be larger than that accounted by the construct. Table 8 shows that all the AVEs are above 0.5, ranging from 0.514 for trust to 0.909 for intention. The result indicates that all the scales reach the required criteria of internal consistency.

Table 7. Item Weights and Loadings				
Construct	**Item**	**Weight**	**Loading**	**T-Statistic***
Control	CON1	.4483	.8036	19.98
	CON2	.4230	.8170	24.41
	CON3	.4116	.7147	13.37
Awareness	PAW1	.3744	.7973	19.89
	PAW2	.4230	.8411	26.13
	PAW3	.4252	.8158	27.27
Collection	COL1	.2602	.7996	24.22
	COL2	.2962	.8472	27.77
	COL3	.3316	.9109	58.35
	COL4	.2958	.8078	26.04
Risk Perception	RSB1	.3129	.8395	38.49
	RSB2	.3276	.9137	69.43
	RSB3	.3454	.9101	70.30
	RSB4	.1928	.6693	11.86
Trust	TRU1	.4812	.7180	18.23
	TRU2	.2617	.7785	20.36
	TRU3	.1689	.7815	13.18
	TRU4	.1426	.7304	12.28
	TRU5	.0963	.6155	7.34
	TRU6	.0887	.5915	6.98
	TRU7	.1491	.6978	10.29
	TRU8	.1023	.3504	12.26
Security Concern	SEC1	.2190	.7665	16.14
	SEC2	.1421	.7699	15.36
	SEC3	.2851	.8338	24.29
	SEC4	.3024	.7907	21.66
	SEC5	.3064	.8065	21.84
Subjective Norm	SN1	.5473	.8375	15.16
	SN2	.6207	.8782	29.01
Attitude	ATT1	.5673	.9525	131.29
	ATT2	.4966	.9331	69.64
Intention	INT1	.5231	.9532	103.77
	INT2	.5257	.9537	98.34

Note: T-Statistics are for loadings, not weights. *All loadings are significant at $p < .001$

Table 8. Internal Consistencies and Correlation of Constructs												
	Comp Reliab	**Alpha**	**CON**	**AWA**	**COL**	**SEC**	**RSK**	**TRU**	**SN**	**PBC**	**ATT**	**INT**
Control (CON)	.823	.732	**.608**									
Awareness (AWA)	.859	.751	.484	**.670**								
Collection (COL)	.907	.856	.351	.501	**.710**							
Security Concern (SEC)	.895	.855	.305	.248	.416	**.630**						
Risk (RSK)	.904	.879	.088	.125	.254	.294	**.704**					
Trust (TRU)	.873	.835	.15	.243	.122	-.088	-.458	**.514**				
Sub Norm (SN)	.848	.789	.202	.196	.103	-.103	-.247	.625	**.736**			
Perceived Behav Con (PBC)	1	1	.000	.009	.017	-.176	-.186	.349	.398	**1**		
Attitude (ATT)	.941	.810	-.026	.031	-.030	-.050	-.525	.586	.366	.219	**.889**	
Intention (INT)	.952	.916	.043	.014	-.066	-.255	-.180	.489	.471	.601	.401	**.909**
Square Root of AVE			**.78**	**.82**	**.84**	**.79**	**.84**	**.72**	**.86**	**1**	**.94**	**.95**

Note: Average Variance Extracted (AVE) is shown on diagonal. Comp Reliab = Composite Reliability. Alpha = Cronbach's Alpha. Perceived Behav Con = Perceived Behavioral Control. Sub Norm = Subjective Norm.

5.1.3 Validity of Constructs

The validity of constructs is important since the latent constructs can not be measured directly and they have to be measured through indicator variables. While using indicators to measure latent constructs it is necessary to ascertain that the scales are capturing the essence of the construct that it is measuring. In general, two elements of construct validity, known as convergent and discriminant validities are examined for latent constructs (Straub et al. 2004). Convergent validity is determined when each measurement item correlates strongly with its related theoretical construct. Discriminant validity is shown when each measurement item correlates weakly with all other constructs except for its theoretically linked construct (Gefen and Straub 2005). This validity indicates the extent to which a given construct is different from other constructs.

Convergent validity is shown when the t-values of the outer model loadings are above 1.96 (Gefen and Straub 2005). As shown above in Table 7, convergent validity for all the constructs is established since the T-values are well above the required level indicating that the items are significantly related to their respective constructs. The results determine that the individual items in presence of other items converged into the construct with which they are theoretically associated.

Discriminant validity can be assessed in two ways (Chin 1998), 1) none of the items should load more highly on another construct than it does on the construct it intends to measure (i.e. loadings should be higher than cross-

loadings), 2) the square root of the average variance extracted (AVE) for each construct should be larger than the inter-construct correlations. The average variance shared between the construct and its indicators should be larger than the variance shared between the construct and other constructs (Fornell and Larcker 1981). In PLS, confirmatory factor analysis (CFA) was done following the method as suggested by (Gefen and Straub 2005). The latent variable scores were calculated and then correlated with the original items. As evident from the results of confirmatory factor analysis (CFA) in Table 9, all indicators load more highly on their own constructs than on other constructs. Table 8 above provides the square root of AVEs and the correlations. As shown by comparing the inter-construct correlations and the square root of AVE above in Table 8, all constructs share more variance with their respective indicators than with other constructs. Hence, these results support the convergent and discriminant validity of the research constructs proposed in the model.

Table 9. Results of Confirmatory Factor Analysis (CFA)										
	Control	**Awareness**	**Collection**	**Security**	**SN**	**Trust**	**Risk**	**PBC**	**Attitude**	**Intention**
CON1	**0.819**	0.510	0.380	0.280	0.177	0.152	0.113	-0.024	0.073	-0.031
CON2	**0.837**	0.421	0.272	0.129	0.169	0.192	0.021	0.025	0.039	0.064
CON3	**0.689**	0.380	0.299	0.237	0.176	0.110	0.052	-0.014	-0.020	0.026
PAW1	0.456	**0.820**	0.340	0.079	0.232	0.200	0.025	0.048	0.035	0.061
PAW2	0.431	**0.833**	0.455	0.229	0.166	0.243	0.143	0.025	0.077	0.085
PAW3	0.481	**0.799**	0.504	0.343	0.141	0.208	0.168	-0.046	0.046	-0.006
COL1	0.252	0.363	**0.820**	0.363	0.038	0.073	0.200	0.047	0.024	-0.024
COL2	0.386	0.412	**0.856**	0.337	0.101	0.216	0.097	-0.021	-0.020	-0.057
COL3	0.412	0.525	**0.909**	0.443	0.085	0.181	0.207	-0.009	0.027	-0.068
COL4	0.305	0.493	**0.810**	0.486	-0.005	0.076	0.225	-0.085	-0.045	-0.117
SEC1	0.198	0.261	0.389	**0.802**	-0.108	-0.075	0.279	-0.170	-0.113	-0.244
SEC2	0.198	0.141	0.343	**0.829**	-0.032	-0.008	0.169	-0.137	-0.011	-0.153
SEC5	0.218	0.216	0.349	**0.780**	-0.195	-0.222	0.427	-0.258	-0.194	-0.316
SEC4	0.228	0.215	0.462	**0.777**	-0.104	-0.004	0.348	-0.044	-0.087	-0.161
SEC3	0.248	0.233	0.394	**0.854**	-0.167	-0.087	0.321	-0.180	-0.109	-0.246
SN1	0.137	0.178	0.006	-0.196	**0.917**	0.512	-0.340	0.381	0.459	0.502
SN2	0.240	0.225	0.096	-0.147	**0.894**	0.612	-0.331	0.401	0.402	0.435
TRA1	0.207	0.281	0.119	-0.173	0.643	**0.779**	-0.409	0.367	0.493	0.515
TRA2	0.297	0.340	0.155	-0.120	0.593	**0.785**	-0.377	0.337	0.457	0.491
TRI1	0.208	0.269	0.140	-0.045	0.498	**0.878**	-0.381	0.256	0.442	0.414
TRI2	0.287	0.298	0.147	-0.078	0.476	**0.854**	-0.342	0.283	0.437	0.407
TRB1	0.060	0.137	0.118	-0.110	0.432	**0.794**	-0.317	0.277	0.419	0.362
TRB2	0.017	0.096	0.138	-0.017	0.473	**0.787**	-0.361	0.269	0.422	0.329
TRB3	0.129	0.175	0.141	-0.075	0.501	**0.849**	-0.343	0.280	0.430	0.387
RSB1	0.094	0.103	0.212	0.458	-0.353	-0.342	**0.747**	-0.196	-0.183	-0.204
RSB2	0.043	0.090	0.170	0.377	-0.276	-0.386	**0.797**	-0.262	-0.172	-0.186
RSB3	-0.036	0.056	0.105	0.284	-0.345	-0.416	**0.780**	-0.272	-0.195	-0.264
RSB4	0.001	0.046	0.134	0.364	-0.332	-0.448	**0.789**	-0.267	-0.193	-0.284
PBC	-0.008	0.012	-0.025	-0.160	0.385	0.305	-0.236	**0.950**	0.324	0.522
ATT1	-0.033	0.063	-0.048	-0.268	0.498	0.600	-0.343	0.481	**0.753**	0.623
ATT2	0.083	0.067	-0.007	-0.214	0.471	0.498	-0.282	0.396	**0.762**	0.585
INT1	-0.017	0.028	-0.104	-0.296	0.444	0.440	-0.220	0.517	0.583	**0.962**
INT2	0.057	0.069	-0.062	-0.239	0.492	0.485	-0.283	0.505	0.584	**0.955**

5.3 Structural Model

After establishing the reliability and validity of the measurement model the hypotheses were tested by examining the structural model. The structural model reflects the hypothesized linkages between the constructs and defines the strengths of the relationships among the constructs. In PLS analysis, the test of the structural model includes estimating the path coefficients, which indicates the strength of the relationships between the predictor and criterion variables, and the sample coefficient of determination or r^2 value, which represents the amount of variance explained by the predictors or independent variables. The assessment of r^2 and path coefficients indicates whether the model is performing well or not. The variance expressed, represented by r^2, is a measure of the predictive power of the model is and it is interpreted in the same way as r^2 in regression analysis (Barclay et al. 1995). To hold the hypothesized relationships, the path coefficients should be significant and they should also be consistent in the direction of relationships as hypothesized in the research model. Since PLS does not directly provide for significance tests for the path coefficients, the bootstrapping resampling procedure was used with 200 samples (Chin 1998). PLS Graph allows for bootstrapping (Efron and Tibshirani 1993) and jackknifing (Gray and Schucany 1972) estimation procedures. The reason for choosing bootstrapping over jackknifing in this study was to get more efficiency without regard to the computational time. Jackknifing, considered as

an approximation to the bootstrap, is viewed as the less efficient of the two (Efron and Tibshirani 1993) .

To investigate the specific hypotheses, t-statistics for the standardized path coefficients were assessed and p-values based on a two-tail test with a significance level of .05 were calculated. All of the relationships except for one were significant. The structural model showed r^2 of 0.53 for intention to transact in e-commerce, r^2 of 0.43 for attitude and R^2 of 0.33 for risk perception as well. The estimation provides support for most of the hypotheses. The results of the PLS estimation is provided in Figure 4. Table 10 displays the path coefficients and summarizes the hypothesis tests.

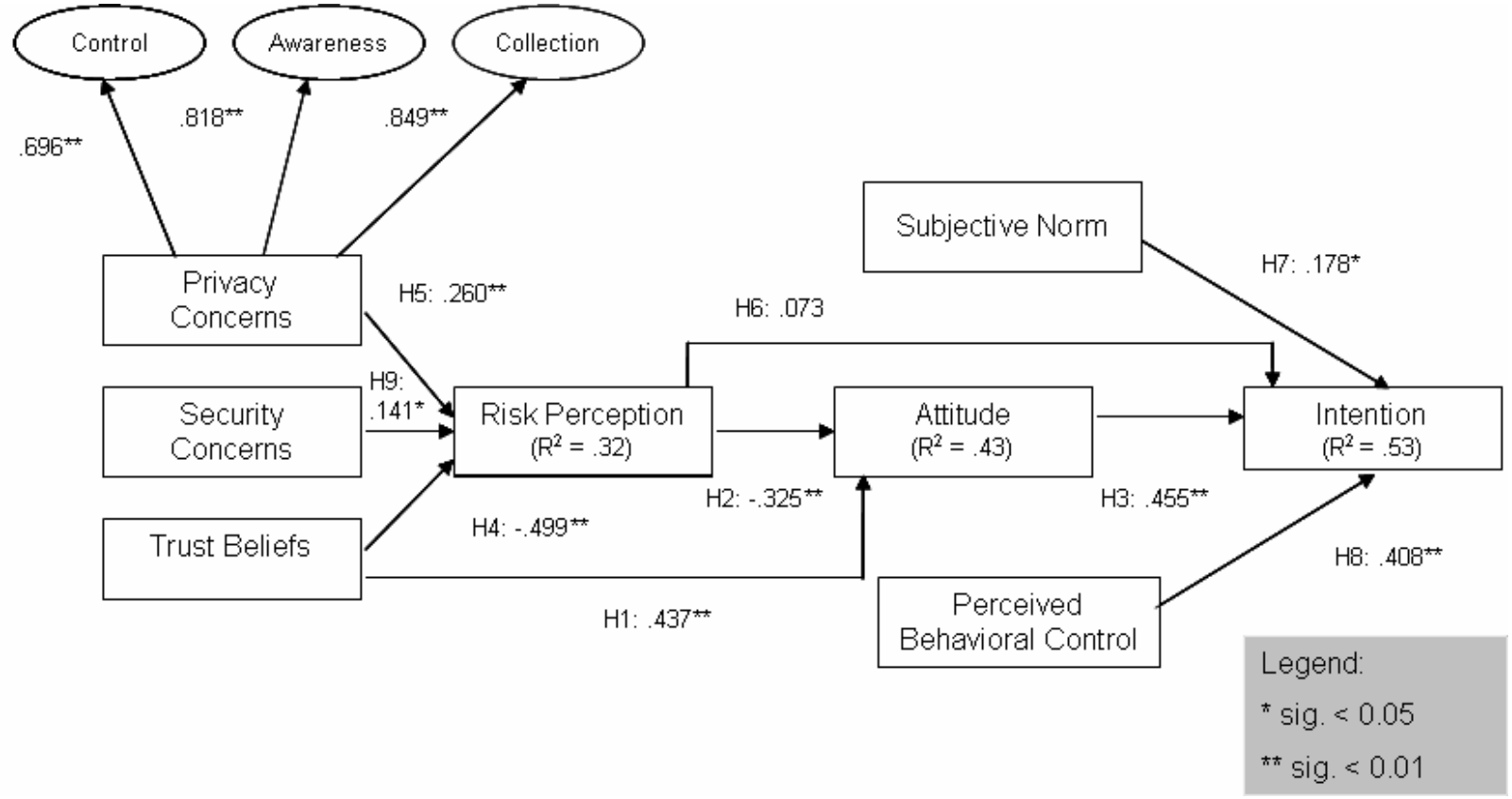

Figure 4. Results of the PLS Analysi

Table 10. Path Coefficients and Summary of Hypothesis Tests				
Paths (Direction)	**Coefficient**	**Standard Error**	**T-statistic**	**Support**
H1) T → ATT (+)	.437	.052	8.39	Yes
H2) RP → ATT (-)	-.325	.055	5.92	Yes
H3) ATT → INT (+)	.455	.081	5.64	Yes
H4) T → RP (-)	-.499	.052	9.58	Yes
H5) PC → RP (+)	.260	.066	3.93	Yes
H6) RP → INT (-)	.073	.054	1.35	No
H7) SN → INT (+)	.178	.064	2.77	Yes
H8) PBC → INT (+)	.408	.073	5.59	Yes
H9) SC → RP (+)	.141	.062	2.28	Yes

Note: T = Trust Beliefs; ATT = Attitude; RP = Risk Perception; INT = Intention; SN = Subjective Norm; PBC=Perceived Behavioral Control; PC = Privacy Concern; SC = Security Concern.

Attitude. As expected in hypothesis 1, trust beliefs had significant effect on attitude ($b = .437$, $t = 8.39$, $p < .01$). The more one trusts an online company the more favorable the attitude towards it. Consistent with hypothesis 2, risk perception had a significant negative effect on attitude ($b = -.325$, $t = 5.92$, $p < .01$). The more risk perceived in an online company will negatively impact the attitude formed towards that company.

Intention. Hypothesis 3 stating the relationship between the attitude and the intention was significant ($b = .455$, $t = 5.64$, $p < .01$). A favorable attitude towards an online company will increase the likelihood of taking part in e-commerce with that company. As predicted in hypothesis 7, subjective norm

had a positive impact on intention (b = .178, t = 2.77, p < .05). A consumer's intention is positively related with the normative beliefs of his/her peer groups and family. Hypothesis 8 was also found significant (b = .408, t = 5.59, p < .01). The more control a consumer feels he/she has, the stronger is his/her intention to engage in an e-commerce transaction.

Risk Perception. The impact of trust beliefs on risk perception of consumers was significant (b = -.499, t = 9.58, p < .01). The direction of the relationship was negative as expected in hypothesis 4. The more trust a consumer has with an online company the lesser will be his/her risk perception. Hypothesis 5 was found significant (b = .260, t = 3.93, p < .01). The more concerned a consumer is regarding his/her privacy the higher level of risk he/she is going to perceive in taking part in e-commerce. Hypothesis 6 indicating the relationship between risk perception and intention was not supported (b = .073, t = 1.35, p > .05). There was no support for the argument that the more risk perception lead to lower intention to transact in e-commerce. It appears that there is a full mediation of attitude in the relationship between risk perception and intention. In other words, there is no direct effect of risk perception on intention. Risk perception influences the attitude and the attitude affects the intention. Attitude is shaped by both risk and trust beliefs. However, hypothesis 9 was supported (b = .141, t = 2.28, p < .05). Similarly to privacy concern, security concern also had a positive impact on risk perception. The

more concerned a consumer is about his/her security, the more risk he/she perceives in taking part in an e-commerce transaction.

CHAPTER 6

DISCUSSION AND CONCLUSION

This research was undertaken to meet three primary objectives: 1) provide a clear delineation of privacy and security concerns, 2) to propose an integrative framework of e-commerce adoption by incorporating privacy and security concerns, risk perception and trust beliefs into the theory of planned behavior and 3) to empirically validate the framework. This chapter provides a discussion of the research findings, limitations, contribution to research, practical implications, future research directions and conclusion.

6.1 Discussion of Findings

Consistent with the proposed research model, the results suggest that privacy and security concerns, and trust beliefs had effects on risk perception. Among these effects, trust had the largest effect followed by privacy and security concerns. Furthermore, risk perception and trust beliefs had effects on attitude. The effect of trust beliefs on attitude was larger than the effect of risk perception on attitude. Similarly, subjective norm, perceived behavioral control and attitude had a positive and direct effect on intention to take part in e-commerce. Among the predictors of intention, attitude was the most influential followed by perceived behavioral control and subjective norm. However, the

effect of risk perception was not found to be significant on intention. The reason for this could be that risk perception only aids in forming attitude of consumers rather than their intentions. Even though the risk perception is high, consumers may not outright decide not to take part in e-commerce. Consumers would also consider the trust beliefs they may have towards online companies and make their purchasing decision. In addition to risk perception, trust beliefs play a significant role in shaping the attitude of consumers. The finding of the insignificant relationship between risk perception and intention support the fact that attitude fully mediates the relationship between risk perception and intention.

The effect of privacy concerns on risk perception was larger than that of security concerns. As the consumers get more experienced and sophisticated using the Web, the security concerns which they may have had at the beginning are not reflected in their risk perceptions. It is likely that they have adopted protective measures on their own to protect their privacy online. An example of such a measure is that of providing false information to online companies.

Privacy concerns of consumers appear to be innate beliefs which do not undergo transformation over time. Even Internet experience does not change these beliefs. Moreover, privacy concerns may likely be bolstered by becoming aware of media coverage on privacy violations in the context of e-commerce.

In contrast to privacy concerns, security concerns are evolutionary beliefs. These beliefs can be transformed over time with more awareness and

Internet experience. As consumers become familiar with ongoing threats of privacy intrusion, such as the uses of information gathering technologies like spyware, malware and adware; they are more likely to adopt protective measures. Such protective measures may be installing and updating firewall, virus definition files, anti-spyware tools et cetera. With the adoption of protective measures, consumers become more confident in taking part in e-commerce since they are able to mitigate their security concerns to some extent.

The effect of trust was the largest among the predictors of risk perception. Online companies develop trust beliefs in consumers by assuring them of their expertise in performing electronic transactions, being fair in its conduct of customer transactions and keeping the customer's best interests in mind. Besides these actions, online companies can also encourage consumers to do business with them by assuring the protection of their personal information. Such measures include the use of trust and security seals on their websites. By developing trust in consumers, online companies are able to compromise the effects of privacy and security concerns to a greater extent and thereby encourage the consumers to take part in e-commerce. Developing trust beliefs is a necessary condition for consumers to participate in e-commerce since the online companies have no opportunities of creating personal relationships as in an offline environment. However, using technologies like personalization and recommendation agents, online companies can create some degree of relationships with consumers. The benefit received by

consumers with use of these technologies may help to bolster the trust beliefs in consumers. For example, consumers may find the recommendations made by the recommendation agents quite helpful in making their decision to buy certain products. In such instances, consumers may develop favorable attitudes toward online companies.

Attitude was affected by trust beliefs and risk perception where the effect of trust beliefs was much larger. It appears that trust beliefs not only have the direct effect on attitude but also indirect effect through risk perception. This can be interpreted as trust impacting attitude not only directly but also indirectly by minimizing the risk perception of consumers. If interpreted along the line of regression analysis, risk perception mediates the relationship between trust beliefs and attitude. This also provides support to the trust and risk framework of Mayer et al. (1995) which postulates risk as the consequences of trust rather than the other way round.

Amongst the predictors of intention, attitude is the most important implying that consumers are most likely to decide to take part in e-commerce based on their favorable opinion of the online company.

6.2 Limitations

The limitations of this study are discussed in this section. The first limitation in this study is the use of student subjects. External validity of a study is based on the subjects and research setting (Cook and Campbell 1979). Since this study took place in an educational setting, its generalizability to general population of consumers lacks to some degree. Most of the criticism towards using student subjects is related to the argument that they differ significantly from the population in their perception regarding the phenomenon of interest. Since the phenomenon of interest in this study is the intention to take part in e-commerce it looks at the subjects from the individual perspective rather than being a part of an organization. Therefore, the limitations to extend results to general population by using student subjects in this study must be viewed in this light. Furthermore, student population, with resources and skills to use the Internet, form a significant pool of the online consumers.

The second limitation of this study is mono-method bias. For one of the constructs, i.e. perceived behavioral control, there was only one measure. While using a single measure there is always the potential threat to construct validity, i.e. not measuring the construct one is supposed to measure. Since this construct is not a key construct central to this research, the limitation should be viewed in this light. Future studies should incorporate multiple measures for all the constructs.

The data for both independent and dependent variables were gathered using self-reports. Common method variance is a common problem related to self-reports (Podsakoff and Organ 1986) because such variance is one of the main sources of measurement error. One-factor test, recommended by Podsakoff and Organ (1986), is the most popular method to test for the presence of common method variance, although it has been criticized for its drawbacks (Podsakoff et al. 2003). The basic assumption of one-factor test is that one single factor will emerge from factor analysis or one single factor will account for the most variance. Conducting one-factor test gave some support that the common method variance may not be a serious problem. However, the results should be taken with caution with regard to the drawbacks of this test. The results are given in Appendix B. It shows that there were 10 factors that emerged instead of one major factor showing that there is no major threat of common method variance. The largest factor accounted for 26.3 of the variance while the second largest factor accounted for 17.7 of the variance.

Another limitation of this study is that respondents got to choose their own online company. This may have bias their responses since they are most likely to choose the companies that they are more familiar with. Future studies should overcome this shortcoming by asking respondents to answer about a specific online company so that all the responses relate to same online company.

6.3 Contribution and Implication

The major contributions of this study are developing and validating an integrative framework of e-commerce adoption at the individual level. The model includes privacy and security concerns, risk perception and trust beliefs. This study also highlighted the distinction of constructs of privacy and security concerns and showed their differential effects on other related constructs in the research model.

Implications of this study follow for both theory development as well as practice. By integrating concerns for privacy and security in the theoretical framework of TPB, this study made a key contribution for theory development. Consumers' concerns influence their different set of beliefs which ultimately decide on the intention and behavior. Besides concerns, this study also introduced the risk perception into the framework of TPB. Since a consumer makes the decision to participate in e-commerce in a social confluence of trust beliefs and risk perception, which in turn is affected by concerns for privacy and security, it is necessary that framework of e-commerce adoption include all these factors. For trust literature, this study contributes by emphasizing the role of risk perception as a consequence of trust beliefs. Further, this study also proposes a direct and indirect effect of trust on attitude through risk perception.

E-commerce adoption studies have been mostly centered on usability features of websites. The major barriers that need to be crossed before consumers reach the level of adoption are the concerns for privacy and

security. This study is one of the first attempts to develop an integrative framework of e-commerce adoption with the constructs of privacy and security concerns.

The managerial implication of this study is that usability features of the website can be enhanced not only aesthetically but also by adding security features. Having security features would help gain the confidence of consumers. Besides, adding other technical features, such as recommendation agents and personalization schemes can help to create favorable attitude in consumers towards their websites. Clear and readable privacy and security policies should be posted on the websites. As consumers become more experienced with their online habits, a simple compromise on privacy and security features may cost a business. Further, shortcomings on securing personal information may even result in serious consequences.

6.4 Future Research and Conclusion

This study addresses the social issues targeted at the initial adoption of e-commerce. Future studies are suggested to incorporate technological measures as suggested by TAM. After consumers cross the initial hurdle of privacy and security concerns their decision to buy products from a specific online company may depend on usability features of their website. In a field study most of the factors can not be controlled thus providing limited information for causality. Future studies should also validate the model by conducting experiments in a controlled manner. In this study, the respondents were asked

to choose an online company and select the product of their own choice. Because of this the effect of risk perception may have been less pronounced, since the subjects would more likely choose an online company that they are more familiar with, or whom they trust. Future studies can improve the study by designing laboratory experiment that would ask subjects to provide responses with regard to a specific online company.

This study should be taken as a progressive step towards finding answers to problems that consumers encounter while participating in e-commerce. A research should be deemed significant if it not only provides solutions but also creates interesting avenues for further research. Author hopes that this research will be able to engender further research in e-commerce research.

APPENDIX A

QUESTIONNAIRE ITEMS

APPENDIX A. Questionnaire Items

Construct	Items
Privacy Concerns - Control	Con1: 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. Con2: Consumer control of personal information lies at the heart of consumer privacy My personal information could be misused when transacting with online companies. Con3: I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction
- Awareness of privacy practices	Paw1: Companies seeking information online should disclose the way the data are collected, processed, and used. Paw2: A good consumer online privacy policy should have a clear and conspicuous disclosure. Paw3: It is very important to me that I am aware and knowledgeable about how my personal information will be used.
- Collection	Col1: It usually bothers me when companies ask me for personal information. Col2: When companies ask me for personal information, I sometimes think twice before providing it. Col3: It bothers me to give personal information to so many people. Col4: I am concerned that companies are collecting too much personal information about me.
Trust Beliefs	Tru1: This online company has the skills and expertise to perform transactions in an expected manner. Tru2: This online company has access to the information needed to handle transactions appropriately. Tru3: This online company is fair in its conduct of customer transactions. Tru4: This online company is fair in its customer service policies following a transaction. Tru5: This online company is open and receptive to customer needs. Tru6: This online company keeps its customers' best interests in mind during most transactions. Tru7: This online company makes good-faith efforts to address most customer concerns. Tru8: Overall, this online company is trustworthy.

APPENDIX A. - continued

Risk Perception	Rsb1: There would be high potential for loss associated with giving information to this online company. Rsb2: It would be risky to give information to this online company. Rsb3: Providing this online company with information would involve many unexpected problems. Rsb4: There would be too much uncertainty associated with providing information to this online company.
Security Concerns	Sec1: I would not feel secure sending sensitive information across the Web. Sec2: The Web is not a secure means through which to send sensitive information. Sec3: I would not feel totally safe providing sensitive information about myself over the Web. Sec4: I think my sensitive information sent to online companies will be accessed by unauthorized parties. Sec5: I hesitate to make purchase from the Web because of security issues of sensitive information.
Attitude	I think buying from the online company in near future would be: 1) Very bad idea / Very good idea 2) Very desirable / Very undesirable
Subjective Norm	SN1: Most people who are important to me would purchase a product from the online company. SN2: Most people who are important to me think that it is fine to purchase a product from the online company.
Perceived Behavioral Control	PCB: Please rate the difficulty while purchasing this product from the online company: Extremely difficult / Extremely easy
Intention	Int1: What is the extent to which you will buy from this online company? Unlikely / Likely Int2: I predict that I would consider buying a product from this online company.

APPENDIX B

FACTOR ANALYSIS

APPENDIX B. Factor Analysis

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	8.680	26.304	26.304	8.680	26.304	26.304	3.765	11.409	11.409
2	5.850	17.728	44.032	5.850	17.728	44.032	3.348	10.145	21.554
3	2.113	6.404	50.436	2.113	6.404	50.436	3.112	9.431	30.984
4	1.905	5.773	56.209	1.905	5.773	56.209	2.908	8.813	39.797
5	1.441	4.367	60.576	1.441	4.367	60.576	2.895	8.774	48.572
6	1.356	4.109	64.685	1.356	4.109	64.685	2.684	8.132	56.704
7	1.071	3.246	67.931	1.071	3.246	67.931	2.145	6.500	63.204
8	0.967	2.929	70.861	0.967	2.929	70.861	1.581	4.792	67.996
9	0.873	2.647	73.508	0.873	2.647	73.508	1.545	4.682	72.678
10	0.856	2.594	76.102	0.856	2.594	76.102	1.130	3.425	76.102
11	0.764	2.316	78.418						
12	0.604	1.830	80.248						
13	0.590	1.788	82.036						
14	0.511	1.549	83.585						
15	0.481	1.457	85.043						
16	0.458	1.388	86.431						
17	0.455	1.378	87.808						
18	0.435	1.317	89.125						
19	0.410	1.242	90.367						
20	0.374	1.135	91.502						
21	0.354	1.074	92.576						
22	0.310	0.940	93.516						

APPENDIX B. - continued

	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
23	0.294	0.892	94.408						
24	0.281	0.852	95.260						
25	0.254	0.770	96.029						
26	0.241	0.730	96.759						
27	0.219	0.663	97.423						
28	0.200	0.606	98.028						
29	0.186	0.565	98.593						
30	0.142	0.429	99.022						
31	0.122	0.369	99.391						
32	0.112	0.339	99.730						
33	0.089	0.270	100.000						

REFERENCES

Agarwal, R., and Karahanna, E. (2000). "Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage." *MIS Quarterly*, 24(4), 665-694.

Ajzen, I. (1985). "From Intentions to Actions: A Theory of Planned Behavior." Action Control: From Cognition to Behavior, J. Kuhl and J. Beckmann, eds., Springer Verlag, New York, 11-39.

Ajzen, I. (1991). "The Theory of Planned Behavior." *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.

Ajzen, I. (2002). "Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior." *Journal of Applied Social Psychology*, 32(4), 665-683.

Ajzen, I., and Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behavior*, Prentice-Hall, Englewood Cliffs, NJ.

Bagozzi, R. P. (1980). *Causal Modeling in Marketing*, John Wiley and Sons, New York.

Barclay, D., Thompson, R., and Higgins, C. (1995). "The Partial Least Squares Approach to Causal Modeling: Personal Computer Adoption and Use as an Illustration." *Technology Studies: Special Issue on Research Methodology*, 2(2), 285-324.

Baroudi, J. J., and Orlikowski, W. J. (1989). "The Problem of Statistical Power in MIS Research." *MIS Quarterly*, 13(1), 86-106.

Bauer, R. A. (1967). "Consumer Behavior as Risk Taking." Risk Taking and Information Handling in Consumer Behavior, D. F. Cox, ed., Harvard University, Boston, MA, 23-33.

Belanger, F., Hiller, J. S., and Smith, W. J. (2002). "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes." *The Journal of Strategic Information Systems*, 11(3-4), 245-270.

Bhattacherjee, A. (2002). "Individual Trust in Online Firms: Scale Development and Initial Test." *Journal of Management Information Systems*, 19(1), 211-241.

Carmines, E. G., and Zeller, R. A. (1979). *Reliability and Validity Assessment*, Sage, Beverly Hills, CA.

Chang, M. K., Cheung, W., and Lai, V. S. (2005). "Literature derived reference models for the adoption of online shopping." *Information & Management*, 42(4), 543-559.

Chellappa, R. K. (2005). "Consumers' Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security." *Working paper*, University of Southern California, Los Angeles, CA.

Chin, W. W. (1998). "The partial least squares approach to structural equation modeling." Modern Methods for Business Research, G. A. Marcoulides, ed., Lawrence Erlbaum Association, London, UK, 295-336.

Churchill, G. A. (1979). "A Paradigm for Developing Better measures of Marketing Constructs." *Journal of Marketing Research (JMR)*, 16(1), 64-73.

Clarke, R. (1999). "Internet Privacy Concerns Confirm the Case for Intervention." *Communications of the ACM*, 42(2), 60-67.

Cohen, J. (1992). "A Power Primer." *Psychological Bulletin*, 112(1), 155-159.

Cook, T. D., and Campbell, D. T. (1979). *Quasi-Experimentation: Design and Analysis Issues for Field Settings*, Houghton Mifflin Company, Boston.

Culnan, M. (2000). "Protecting privacy online: Is self-regulation working?" *Journal of Public Policy & Marketing*, 19(1), 20-26.

Culnan, M., and Armstrong, P. (1999). "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation." *Organization Science*, 10(1), 104-115.

Culnan, M. J. (1993). "How did they get my name - An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use." *MIS Quarterly*, 17(3), 341-361.

Culnan, M. J., and Bies, R. J. (1999). "Managing Privacy Concerns Strategically: The Implications of Fair Information Practices for Marketing in the Twenty-first Century." Visions of Privacy: Policy Choices for the Digital Age, C. J. Bennett and R. Grant, eds., University of Toronto Press, Toronto, ON, 149-167.

Davis, F. D. (1989a). "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology." *MIS Quarterly*, 13(3), 318-340.

Davis, F. D. (1989b). "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology." *MIS Quarterly*, 13(3), 318-340.

Dhillon, G., Bardacino, J., and Hackney, R. "Value Focused Assessment of Individual Privacy Concerns for Internet Commerce." *Proceedings of the Twenty Third International Conference on Information Systems*, Barcelona, Spain.

Dinev, T., and Hart, P. "Privacy Concerns and Internet use - A Model of Trade-Off Factors." *Academy of Management Conference*, Seattle, WA.

Dommeyer, C. J., and Gross, B. L. (2003). "What Consumers Know and What They Do: An Investigation of Consumer Knowledge, Awareness, and Use of Privacy Protection Strategies." *Journal of Interactive Marketing*, 17(2), 34-51.

Earp, J. B., Anton, A. I., and Jarvinen, O. "A Social, Technical, and Legal Framework for Privacy Management and Policies." *Eight Americas Conference on Information Systems*, Dallas, TX, 605-612.

Efron, B., and Tibshirani, R. J. (1993). *An Introduction to the bootstrap*, Chapman and Hall, New York.

Fishbein, M. (1967). "Attitude and the prediction of behavior." Readings in Attitude Theory and Measurement, M. Fishbein, ed., Wiley, New York.

Fishbein, M., and Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*, Addison-Wesley, Reading, MA.

Fornell, C., and Bookstein, F. L. (1982). "Two Structural Equation Models: LISREL and PLS Applied to Consumer Exit-Voice Theory." *Journal of Marketing Research (JMR)*, 19(4), 440-452.

Fornell, C., and Larcker, D. F. (1981). "Evaluating Structural Equation Models With Unobservable Variables and Measurement Error." *Journal of Marketing Research*, 18(1), 39-50.

Foxman, E. R., and Kilcoyne, P. (1993). "Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues." *Journal of Public Policy & Marketing*, 12, 106-119.

Gefen, D., Karahanna, E., and Straub, D. W. (2003). "Trust and TAM in Online Shopping: An Integrated Model." *MIS Quarterly*, 27(1), 51-90.

Gefen, D., and Straub, D. (2005). "A Practical Guide to Factoral Validity using PLS-Graph: Tutorial and Annotated Example." *Communications of AIS*, 16, 91-109.

Gefen, D., Straub, D. W., and Boudreau, M.-C. (2000). "Structural Equation Modeling and Regression: Guidelines for Research Practice." *Communications of AIS*, 4(7), 1-78.

Goodhue, D., Lewis, W., and Thompson, R. "PLS, Small Sample Size, and Statistical Power in MIS Research." *Proceedings of the 39th Hawaii International Conference on System Sciences*, Hawaii, 1-10.

Gopal, A., Bostrom, R. P., and Chin, W. W. (1992). "Applying Adaptive Structuring Theory to Investigate the Process of Group Support Systems Use." *Journal of Management Information Systems*, 9(3), 45-69.

Gray, H. L., and Schucany, W. R. (1972). *The Generalized Jackknife Statistic*, Marcel Dekker, New York.

Gray, P. (1999). "Protecting Privacy and Security of Personal Information in the Global Electronic Marketplace." Http://www.ftc.gov/bcp/icpw/comments/ico2.htm.

Greenaway, K. E., and Chan, Y. E. (2005). "Theoretical Explanations for Firms' Information Privacy Behaviors." *Journal of Association for Information Systems*, 6(6), 171-198.

Hagel, J., and Rayport, J. F. (1997). "The Coming Battle for Customer Retention." *Harvard Business Review*, 75(1), 53-65.

Hair, J. F., Tatham, R. L., and Anderson, R. E. (2002). *Multivariate data analysis*, Prentice Hall PTR, Upper Saddle River, N.J.; London.

Harris, I. (2001). "Why Some Companies are trusted and others are not: Personal Experience and Knowledge of Company More Important than Glitz." http://www.harrisinteractive.com/harris_poll/index.asp?PID=237.

Henderson, S. C., and Snyder, C. A. (1999). "Personal information privacy: implications for MIS managers." 36(4), 213.

Hoffman, D., Novak, T., and Peralta, M. (1999a). "Building Consumer Trust Online." *Communications of the ACM*, 42(4), 80-85.

Hoffman, D. L., Novak, T. P., and Peralta, M. A. (1999b). "Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web." *Information Society*, 15(2), 129-139.

Hosmer, L. T. (1995). "Trust - the Connecting Link between Organizational Theory and Philosophical Ethics." *Academy of Management Review*, 20(2), 379-403.

Hulland, J. (1999). "Use of partial least squares (PLS) in strategic management research: A review of four recent." *Strategic Management Journal*, 20(2), 195-209.

Jarvenpaa, S. L., Tractinsky, N., Saarinen, L., and Vitale, M. (1999). "Consumer Trust in an internet store: a cross-cultural validation." *Journal of Computer-Mediated Communication*, 5(2).

Jarvenpaa, S. L., Tractinsky, N., and Vitale, M. (2000). "Consumer trust in an internet store." *Information Technology and Management*, 1(1-2), 45-71.

Joreskog, K. G., and Sorbom, D. (1986). "LISREL VI: Analysis of Linear Structural Relationships by Maximum Likelihood and Least Squares Methods." Scientific Software, Inc., Mooresville, IN.

Karahanna, E., Straub, D. W., and Chervany, N. L. (1999). "Information technology adoption across time: A cross-sectional comparison of pre-adoption and post-adoption beliefs." *Mis Quarterly*, 23(2), 183-213.

Kerlinger, F. N. (1964). *Foundations of Behavioral Research*, Holt, Rinehart, and Winston, New York.

Kim, W. C., and Mauborgne, R. A. (1993). "Procedural Justice, Attitudes, and Subsidiary Top Management Compliance with Multinationals' Corporate Strategic Decisions." *Academy of Management Journal*, 36(3), 502-526.

Kimery, K. M., and McCord, M. (2002). "Third-party Assurances: Mapping the Road to Trust in E-retailing." *Journal of Information Technology Theory and Application*, 4(2), 63-81.

Liu, C., Marchewka, J., Lu, J., and Yu, C. (2004). "Beyond concern: a privacy-trust-behavioral intention model of electronic commerce." *Information & Management*, 42(1), 127-142.

Lohmoller, J. B. (1989). *Latent Variable Path Modeling with Partial Least Squares*, Springer-Verlag, New York.

Luhmann, N. (1979). *Trust and Power*, John Wiley & Sons, Chichester, England.

Lunt, P. (1999). "The electronic consumer: www.confidence." *Consumer Policy Review*, 9(6), 225-229.

Luo, X. (2002). "Trust Production and Privacy Concerns on the Internet A Framework Based on Relationship Marketing and Social Exchange Theory." *Industrial Marketing Management*, 31(2), 111-118.

Malhotra, N. K., Kim, S. S., and Agarwal, J. (2004). "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model." *Information Systems Research*, 15(4), 336-355.

Mayer, R. C., Davis, J. H., and Schoorman, F. D. (1995). "An Integrative Model of Organizational Trust." *Academy of Management Review*, 20(3), 709-734.

McAllister, D. J. (1995). "Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations." *Academy of Management Journal*, 38(1), 24-59.

McKnight, D., Cummings, L. L., and Chervany, N. L. (1998). "Initial Trust Formation in New Organizational Relationships." *Academy of Management Review*, 23(3), 473-490.

McKnight, D. H., Choudhury, V., and Kacmar, C. (2002a). "Developing and validating trust measures for e-commerce: An integrative typology." *Information Systems Research*, 13(3), 334-359.

McKnight, D. H., Choudhury, V., and Kacmar, C. (2002b). "The impact of initial consumer trust on intentions to transact with a web site: a trust building model." *The Journal of Strategic Information Systems*, 11(3-4), 297-323.

Milne, G. (2000). "Privacy and ethical issues in database/interactive marketing: A research framework and overview of the special issue." *Journal of Public Policy and Marketing*, 19(1), 1-6.

Milne, G., and Culnan, M. (2002). "Using the content of online privacy notices to inform public policy: A longitudinal analysis of the 1998-2001 US web surveys." *INFORMATION SOCIETY*, 18(5), 345-359.

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

Nunnally, J. (1978). *Psychometric theory*, McGraw-Hill, New York.

Olivero, N., and Lunt, P. (2004). "Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control." *Journal of Economic Psychology*, 25(2), 243-262.

Pavlou, P. A. (2002). "Institution-based trust in interorganizational exchange relationships: the role of online B2B marketplaces on trust formation." *The Journal of Strategic Information Systems*, 11(3-4), 215-243.

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

Pavlou, P. A., and Fygenson, M. (2006). "Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior." *MIS Quarterly*, 30.

Pavlou, P. A., and Gefen, D. (2004). "Building effective online marketplaces with institution-based trust." *Information Systems Research*, 15(1), 37-59.

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

Pitkow, J., and Kehoe, C. (1997). "GVU's seventh www user survey." Http://www.gvu.gatech.edu/user_surveys/survey-1997-04/.

Podsakoff, P. M., MacKenzie, S. B., Jeong-Yeon, L., and Podsakoff, N. P. (2003). "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies." *Journal of Applied Psychology*, 88(5), 879-903.

Podsakoff, P. M., and Organ, D. W. (1986). "Self-reports in Organizational Research: Problems and Prospects." *Journal of Management*, 12(4), 69-82.

Roberts, K. H., and O'Reilly, C. A. (1974). "Failures in Upward Communication in Organizations: Three Possible Culprits." *Academy of Management Journal*, 17(2), 205-215.

Rose, G. M., Khoo, H. M., and Straub, D. W. (1999). "Current Technological Impediments to Business-to-Consumer Electronic Commerce." *Communications of the Association for Information Systems*, 1, 1-74.

Ruppel, C., Underwood-Queen, L., and Harrington, S. J. (2003). "E-commerce: The Roles of Trust, Security, and Type of e-commerce Involvement." *e-Service Journal*, 2(2), 25-45.

Salisbury, W. D., Pearson, R. A., Pearson, A. W., and Miller, D. W. (2001). "Perceived security and World Wide Web purchase intention." *Industrial Management & Data Systems*, 101(3-4), 165-176.

Sambamurthy, V., and Chin, W. W. (1994). "The Effects of Group Attitudes Toward Alternative GDSS Designs on the Decision-making Performance of Computer-Supported Groups." *Decision Sciences*, 25(2), 215-241.

Saunders, C. (2004). "Consumers Confidence Increasing in E-Commerce, Despite Threats." Http://www.ecommerce-guide.com/news/trends/article.php/3440101.

Sheehan, K. B., and Hoy, M. G. (2000). "Dimensions of privacy concern among online consumers." *Journal of Public Policy & Marketing*, 19(1), 62-73.

Sheppard, B. H., Hartwick, J., and Warshaw, P. R. (1988). "The Theory of Reasoned Action: A Meta-Analysis of Past Research with Recommendations for Modifications and Future Research." *Journal of Consumer Research*, 15(3), 325-343.

Sheth, J. N., and Venkatesan, M. (1968). "Risk-Reduction Processes in Repetitive Consumer Behavior." *Journal of Marketing Research*, 5(3), 307-310.

Singh, T., and Hill, M. E. (2003). "Consumer Privacy and the Internet in Europe: a View from Germany." *Journal of Consumer Marketing*, 20(7), 634-651.

Sitkin, S. B., and Pablo, A. L. (1992). "Reconceptualizing the Determinants of Risk Behavior." *Academy of Management Review*, 17(1), 9-38.

Smith, H. J., Milberg, S. J., and Burke, S. J. (1996). "Information privacy: Measuring individuals' concerns about organizational practices." *MIS Quarterly*, 20(2), 167-196.

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

Straub, D., Boudreau, M.-C., and Gefen, D. (2004). "Validation Guidelines For IS Positivist Research." *Communications of AIS*, 2004(13), 380-427.

Straub, D. W. (1989). "Validating Instruments in MIS Research." *MIS Quarterly*, 13(2), 146-169.

Suh, B., and Han, I. (2003). "The impact of customer trust and perception of security control on the acceptance of electronic commerce." *International Journal OF Electronic Commerce*, 7(3), 135-161.

Taylor, S., and Todd, P. A. (1995). "Understanding Information Technology Usage - a Test of Competing Models." *Information Systems Research*, 6(2), 144-176.

Udo, G. J. (2001). "Privacy and Security Concerns as Major Barriers for E-commerce: a Survey Study." *Information Management & Computer Security*, 9(4), 165-174.

van der Heijden, H., Verhagen, T., and Creemers, M. (2003). "Understanding Online Purchase Intentions: Contributions from Technology and Trust Perspectives." *European Journal of Information Systems*, 12(1), 41.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. (2003). "User Acceptance Of Information Technology: Toward A Unified View." *MIS Quarterly*, 27(3), 425-478.

Vijayasarathy, L. R. (2004). "Predicting consumer intentions to use on-line shopping: the case for an augmented technology acceptance model." *Information & Management*, 41(6), 747-762.

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

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

Wasko, M. M., and Faraj, S. (2005). "Why should I share? Examining social capital and knowledge contribution in electronic networks of practice." *MIS Quarterly*, 29(1), 35-57.

Webster, J., and Martocchio, J. J. (1992). "Microcomputer Playfulness - Development of a Measure with Workplace Implications." *MIS Quarterly*, 16(2), 201-226.

Werts, C. E., Linn, R. L., and Joreskog, K. G. (1974). "Interclass Reliability Estimates: Testing Structural Assumptions." *Educational and Psychological Measurement*, 34, 25-33.

Wold, H. (1982). "Systems Under Indirect Observation using PLS." A Second Generation of Multivariate Analysis, C. Fornell, ed., Praeger, New York, 325-347.

Xu, H., and Teo, H.-H. "Alleviating Consumers' Privacy Concerns in Location-Based Services: A Psychological Control Perspective." *Proceedings of the Twenty-Fifth International Conference on Information Systems*, Washington, D. C., 793-806.

Yang, Z., and Jun, M. (2002). "Consumer Perception of E-service Quality: From Internet Purchaser and Non-purchaser Perspectives." *Journal of Business Strategies*, 19(1), 19-41.

Zaheer, A., McEvily, B., and Perrone, V. (1998). "Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance." *Organization Science*, 9(2), 141-159.

BIOGRAPHICAL INFORMATION

The author received his doctorate in Information Systems from The University of Texas at Arlington in May 2006. He holds MBA degrees majoring in Computer Information Systems and Finance. He has over seven years of work experience in different industries. His research interests focus on IT organizations, information security and e-commerce. Other research areas include impact of information technology on organizational structure, culture, and value chains and the social aspect of business computing. He is a member of Association for Information Systems (AIS), Decision Sciences Institute (DSI) and Association for Computing Machinery (ACM). His publications have appeared in various journals and conference proceedings.