Antecedents of Online Trust and Acceptance of E-Commerce

Amber C. Hwang, Capella University, Minneapolis, MN 55402, USA; E-mail: amber.hwang@metavante.com
Terence T. Ow, Marquette University, Milwaukee, WI 53201, USA; E-mail: terence.ow@marquette.edu
Veronica D. Hinton-Hudson, University of Louisville, Louisville, KY 40292, USA; E-mail: hintonhudson@louisville.edu

INTRODUCTION

The impact of computer technology has transformed business practices and creation of e-commerce, such as online retailers. However, consumers tend to be reluctant to provide personal information to Web sites because they are unsure if they can fully trust online merchants. Consumer tends to feel uncomfortable engaging in a transaction over the internet with unfamiliar vendors (Gefen and Straub 2002). Previous research has also found that 95% of the consumers have declined to provide personal information to websites because of the lack of trust on those collecting the data (Hoffman at al. 1999, p. 82). McKnight et al. (2002) assert that there is another perception of technology beyond the widely accepted technology acceptance model (TAM). Hence, the trust issue is rooted in security and privacy which has been labeled a key concern of e-commerce by consumers (Miyazaki and Fernadez, 2000). In this study, we build upon the research proposed by McKnight et al. (2002) on understanding the antecedents of trust. We explore factors such as consumers' perceptions of information security, privacy, trust, and their acceptance of e-commerce. Specifically, we are examining the effects of having a third party organization/web seal, and also privacy and security statements on the adoption behavior of electronic commerce.

THEORETICAL BACKGROUND

Trust, according to Pavlou (2001), in electronic transactions context is defined as the subjective probability that customers believe an organization's technology infrastructure and control mechanisms are capable of carrying out transactions that are meeting customers' expectations. Other researchers have included trust as an additional construct in TAM and their findings demonstrated the relationship between trust and adoption intention (McCloskey, 2006; Dahlberg, Mallat, & Oorni, 2003; Pavlou, 2003; Suh & Han, 2003; Keat & Mohan, 2004). McKnight et al. (2002) discusses various forms of trust issues e.g. initial trust, institutional-based trust, trust-related behaviors including trusting intentions and trusting beliefs. Trusting beliefs is defined as the confidence perception that a vendor has attributes that are beneficial to the consumer. These beliefs are competence, benevolence and integrity (Battacherjee 2002, Gefen 1997, Mayer et al. 1995). Trusting intention on the other hand, refers to the willingness to depend on the vendor. There is an element of "volitional preparedness" to make a consumer vulnerable to the vendor (McKnight et al. 2002).

The objective of e-commerce security is information assurance, which means to maintain confidentiality (privacy), integrity, and availability of information resources for authorized organizations and users (Warkentin, Davis, & Bekkering, 2004). Ensuring security and confidentiality are the fundamental prerequisites before any electronic transactions involving sensitive information can take place (Jayawardhena and Foley, 2000). Many researchers have discussed the element of e-commerce security control requirements (Hutchinson & Warren, 2003; Suh & Han, 2003; Kesh and Ramanujan, 2004). These security elements can be summarized in five categories. They are: authentication, non-repudiation, data integrity, confidentiality, and privacy protection.

Researchers have also found that stable situation-specific personal characteristics such as personal innovativeness in information technology (Agarwal and Prasad, 1998) and risk tolerance such as perceived risk (Lu, Hsu, and Hsu, 2005) influence how individuals perceive information technology. Agarwal and Prasad (1998) define personal innovativeness in the domain of information technology (PIIT) as the "willingness of an individual to try out any new information technology." (p.206). They argue that inclusion of personal innovativeness with respect to information technology acceptance model would help to further understand how perceptions are formed and the subsequent role they play in the formation of usage intentions.

Another personality characteristic, perceived risk has been described as comprising the subjective perception of two components: (1) the amount at stake and (2) the degree of certainty about possible negative consequences. Perceived risks can take many forms, depending on the product and consumer characteristics. Lu, Hsu, and Hsu (2005) incorporated perceived risk in their study about intention to use online applications and concluded that perceived risk plays the key factor in influencing the determinants of online applications adoption.

CONCEPTUAL DEVELOPMENT

Figure 1 shows the proposed research model. We are examining the effects of perceived security, the use of privacy and security statements and third part organization seal while controlling the effects of personal characteristics and organization characteristics on trusting beliefs. Then, we study how these trusting beliefs will affect consumers in engaging e-commerce transactions.

Third Party Organization/Web Seal

To address issues of privacy and trust related to on-line transactions, e-commerce assurance services were created in the 1990s (Wakefield & Whitten, 2006). Third party organizations such as Better Business Bureau®, TRUSTe®, and VeriSign ® are organized to promote trust in e-commerce. Studies found that third party web seal promotes consumers feelings of trust (Palmer, Bailey, & Faraj, 2000; Schneiderman, 2000; Wakefield & Whitten, 2006) and confidence in their e-commerce transactions. Thus, the following hypothesis is proposed:

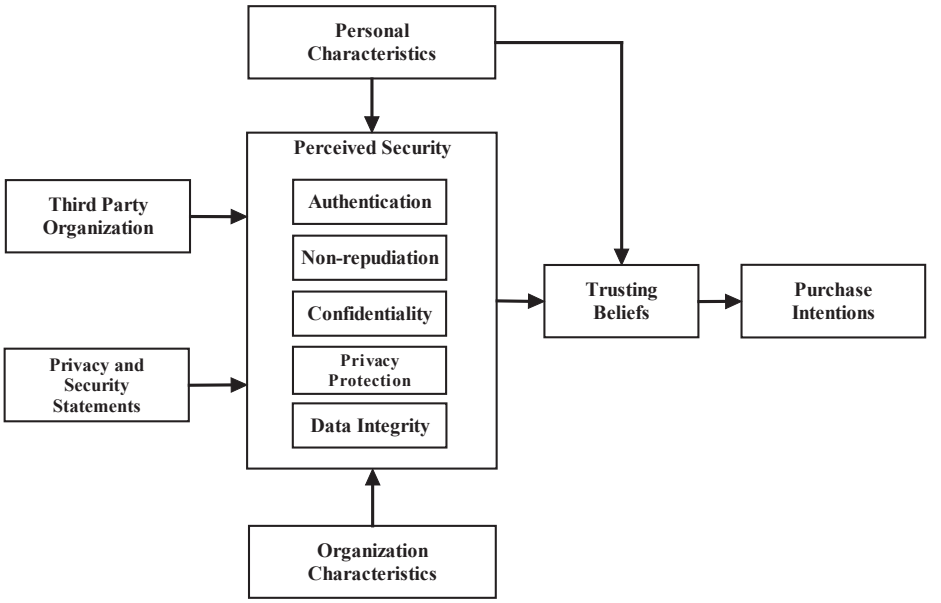
H1: The presence of third party web seal logo has a positive effect on consumers' trust in e-retailer.

Privacy and Security Statements

The ability to monitor and record Internet users' personal information has raised fears about online privacy. According to Federal Trade Commission (FTC) 2000 survey about online privacy, the survey result indicates that 97% of the random sample websites and 99% of the most popular websites collect an e-mail address or some other type of personal information (Federal Trade Commission, 2000). Companies have the ability to collect and follow users' every movement on the Internet by using "cookies" and advanced browser technology. Consumers are concerned about the type of information that is gathered and how this information is being used, and by whom.

Unlike the European countries, where there are laws governing and protecting consumers from being victims of privacy-violating businesses, the United States advocated self-regulation for the Internet. It suggested that businesses should develop and post clearly written policies that inform consumers about who is collecting their personal information and the intended purpose for the collected information. Businesses should also provide consumers with a readily available, simple, and affordable option for exercising their choices with respect to whether and how their personal information is used (Privacy in electronic communications, 1998). Thus, the following hypothesis is proposed for investigation:

Figure 1. Proposed research model



H2: Displaying a privacy and security link on an on-line retailer's home page has a positive effect on consumers' trust in e-retailer.

Perceived Security

Kesh et al. (2002) and Gupta et al. (2004) describe the need of authentication is to "ensure that the origin of an electronic message is correctly identified" (p. 150). The essence of authentication is to make sure the sender of the message or originator of the transaction is the person who he/she claims to be. Authentication reduces the risk of identity theft and fraudulent activities. Non-repudiation refers to the need to ensure that the customers can be certain that they are communicating with the genuine merchant, or vice versa, and each party involved in a transaction will not later falsely deny the transaction (Gupta et al., 2004; Hutchinson & Warren, 2003). Data integrity ensures that only authorized individuals can make changes to the documents transmitted over the network. Integrity ensures the content of the sent message or transaction is the same message or transaction when it is received. Information confidentiality refers to protecting customers' private and personal information to ensure the information is secured and hidden wherever the information is stored, as well as in transit through the Internet. Thus, the following hypotheses are proposed for investigation:

H3: Perceived strength of security has a positive effect on consumers' trust in e-retailer.

Methodology

Instrument Development

Data was collected using a self-administrated questionnaire. Each item presented a statement to which respondents were asked to weigh their level of agreement. All items were measured on a seven-point Likert scale. The measurement items used in this study were derived from validated scales found in previous extant literature, with modified wording to be specific to this study.

Measures for the sub-dimensions of perceived security (SECURITY) were taken from Suh and Han (2003) with modified wordings to adapt the items to the current topic. Measures for antecedents to perceived security were built upon relevant literature. Perceived reputation (PREP) and firm size (PSZE) were derived from Jarvenpaa and Tractinsky (1999). Third-party seal (PTP) and privacy statement perception (GPSS) were modified from Wakefield and Whitten (2006), the privacy statement availability (PPSS) was newly developed items. We differentiated the two based on perception of importance of privacy statement and the availability and presence of such statements. Computer self-efficacy (SEFF), or the confidence and capability of the respondent to use the Internet to make a purchase, was derived from Taylor and Todd (1995). Personal Internet innovativeness (PINN), or the level of respondents' enthusiastic trying out new information technologies and Internet features, was originated from Agarwal and Prasad (1998). Perceived risk (PRSK) was assessed with four items following Jarvenpaa, Tractinsky, and Vitale (1999). These items measured the respondents' perception of there being risk in participating in using online website to make purchase. The measures for trust (TRUST) were based on Pavlou and Gefen (2004). The measures for purchase intention (PINT) sub-dimensions were borrowed and modified from Schlosser, White and Lloyd's (2006) research about online purchase intention.

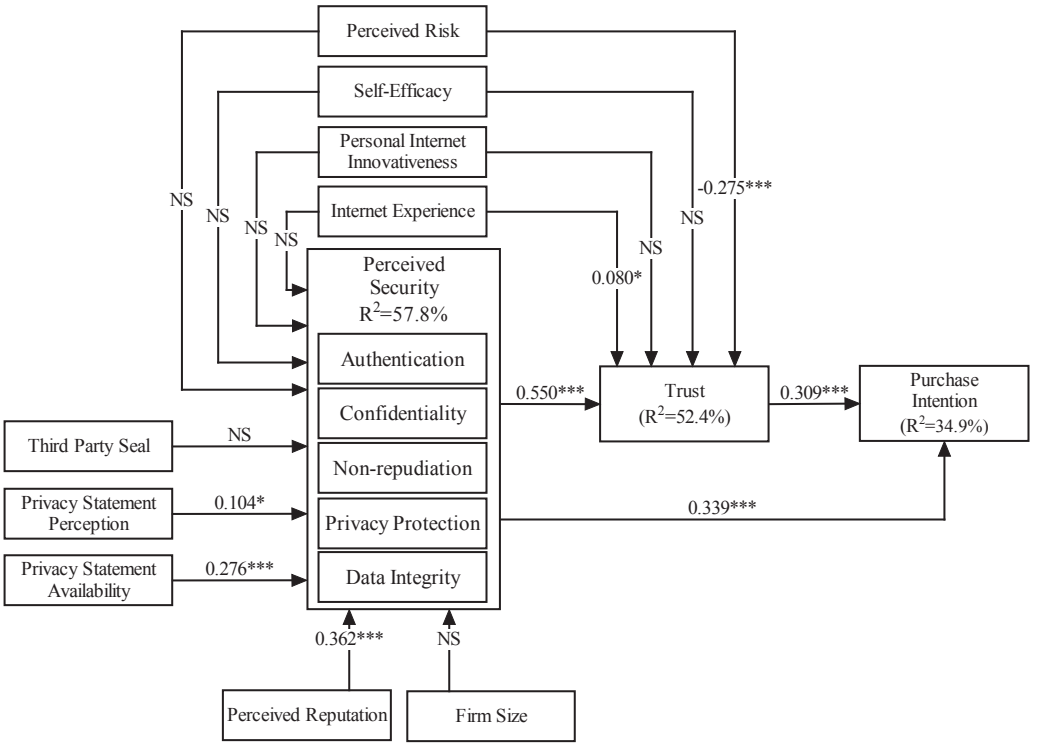
Data Collection

The pool of respondents came from a panel maintained by an online marketing research firm. Invitations were sent out to 4000 panel members. The survey first asked participants to enter the names of three online retailing websites from which they have made a purchase in the past. We randomly picked one entered website and asked participants to answer a series of questions about their impressions of that website. The survey was left open for 14 days. After removing incomplete surveys and surveys that were completed at impossible speed (< 5 minutes), 330 responses were deemed usable giving 8.25% effective response rate. One possible explanation for the low response rate was that there was no reminder e-mail send out to the panel members to remind them to complete the survey. Overall demographic profile of usable respondents: 56% are male with average income of $48,000.

DATA ANALYSIS

From the path model shown in Figure 2, we were able to show strong significance of the availability and presence privacy statements in the perception of security. McKnight et al. (2002) refers to this perception as institutional based trust. Moderate significance was found instead for the perceptions of the importance of these statements. This implies that even though consumers indicate that privacy statements were fairly important, their actions were otherwise, i.e. given the presence

Figure 2. Integrated results of path model



and easily available statements on privacy, it affected their security perception. Perceived reputation is found to be significant in affecting the respondents' perception of perceived security while the presence of third party seal did not influence in their perceptions. The combination of the reputation and third party seal lead us to believe that it is still very important for new websites to develop their reputation and simply putting "artifacts" such as third party seal will not increase the perception of security.

In examining the antecedents for TRUST (Trust in retail website), it is interesting to note that personal characteristics such as innovativeness and self efficacy do not affect TRUST while SECURITY was found to be strongly related to TRUST. In examining the antecedents of purchase intention (PINT), we found significance of both TRUST and SECURITY.

We were able to use Baron and Kenney (1986) method in examining mediating effects. We found that personal characteristics such as perceived risk and internet experience are both mediated by TRUST in purchase intention. Furthermore, we found that signals of privacy statements (GPSS, PPSS) are also mediated by SECURITY to TRUST.

CONCLUSIONS

Based on the data that we analyzed, our research improves on the model suggested by McKnight et al. (2002). We show the antecedents to the institutional based trust model represented by perceived security. We are also able to show the mediating effects of both perceived security and trust for personal characteristics and privacy signals in explaining purchase intention.

REFERENCES

References and working paper is available from terence.ow@marquette.edu

Table 1. Regression model for perceived security

Variables	Unstandardized Coefficients		Standardized Coefficients	t-stats	Significance	VIF
	B	Std. Error	Beta			
PTP	.261	.208	.059	1.251	.212	1.697
GPSS	.475	.220	.104	2.161	.031	1.772
PPSS	1.384	.251	.276	5.513	.000	1.906
PINN	.237	.220	.054	1.079	.282	1.907
SEFF	.266	.213	.060	1.248	.213	1.781
PRSK	-.224	.140	-.065	-1.606	.109	1.229
PREP	1.441	.225	.362	6.412	.000	2.416
PSZE	.278	.252	.056	1.106	.270	1.978
IEXP	-.307	.593	-.019	-.517	.605	1.068