ELSEVIER

Journal of Strategic Information Systems 11 (2002) 245–270

Strategic Information Systems

www.elsevier.com/locate/jsis

Trustworthiness in electronic commerce: the role of privacy, security, and site attributes

France Belanger*, Janine S. Hiller[1], Wanda J. Smith[2]

Center for Global Electronic Commerce, Pamplin College of Business, Virginia Polytechnic Institute and State University, 3007 Pamplin, Blacksburg, VA 24061-0101, USA

Abstract

While the growth of business-to-consumer electronic commerce seems phenomenal in recent years, several studies suggest that a large number of individuals using the Internet have serious privacy concerns, and that winning public trust is the primary hurdle to continued growth in e-commerce. This research investigated the relative importance, when purchasing goods and services over the Web, of four common trust indices (i.e. (1) third party privacy seals, (2) privacy statements, (3) third party security seals, and (4) security features). The results indicate consumers valued security features significantly more than the three other trust indices. We also investigated the relationship between these trust indices and the consumer's perceptions of a marketer's trustworthiness. The findings indicate that consumers' ratings of trustworthiness of Web merchants did not parallel experts' evaluation of sites' use of the trust indices. This study also examined the extent to which consumers are willing to provide private information to electronic and land merchants. The results revealed that when making the decision to provide private information, consumers rely on their perceptions of trustworthiness irrespective of whether the merchant is electronic only or land and electronic. Finally, we investigated the relative importance of three types of Web attributes: security, privacy and pleasure features (convenience, ease of use, cosmetics). Privacy and security features were of lesser importance than pleasure features when considering consumers' intention to purchase. A discussion of the implications of these results and an agenda for future research are provided.
© 2002 Elsevier Science B.V. All rights reserved.

Keywords: Electronic commerce; Security; Privacy; Trust; Business-to-consumer electronic commerce; Web shopping

* Corresponding author. Tel.: +540-231-6720.
E-mail addresses: belanger@vt.edu (F. Belanger), jhiller@vt.edu (J.S. Hiller), wjsmith@vt.edu (W.J. Smith).
[1] Tel.: +540-231-7346.
[2] Tel.: +540-231-6105.

0963-8687/02/$ - see front matter © 2002 Elsevier Science B.V. All rights reserved.
PII: S0963-8687(02)00018-5

1. Introduction

Recently, scholars and practitioners in the field of e-commerce have generated a compelling list of Web attributes that engender trustworthiness (Cassell and Bickmore, 2000; Friedman et al., 2000; Urban et al., 2000). For example, one commonly cited study has identified six features of Web sites that enhance consumer perceptions of the marketer's trustworthiness (Cheskin and SA, 1999). These Web features include: (1) safeguard assurances, (2) the marketers' reputation, (3) ease of navigation, (4) robust order fulfillment, (5) the professionalism of the Website, and (6) the use of state-of-the-art Web page design technology. Beyond capturing these important Web features, Cheskin and SA argue that the 'first and most necessary step' in establishing consumer trust is providing assurances that the consumers' personal information will be safeguarded (p. 10). Many other scholars have reinforced this belief asserting that only after security concerns have been addressed will consumers consider other Web features (i.e. reputation, ease of navigation, transaction integrity) to determine the extent to which they can trust and/or feel comfortable transacting with the marketer (Dayal et al., 1999; Hoffman et al., 1999; Ovans, 1999). Yet, it is unknown which indicators of trustworthiness (third party seals, privacy and security statements) work best or are valued more by consumers.

It is important to understand the factors that might influence consumers' intentions to use this mode of interacting with businesses. As discussed, one factor that is recognized as key for the continued growth of e-commerce is trust (Ba, 2001; Houston, 2001; Jarvenpaa et al., 2000). Congruent with this, this study investigates trust in consumer-oriented e-commerce. If transaction-oriented e-commerce is to be successful, the parties involved must properly assess the level of trust they should have in each other. For example, many potential consumers are reluctant to provide personal information such as credit card numbers to electronic commerce outlets. Clearly, one partner's lack of trust in the other may lead to reluctance to engage in the transaction. According to one study of 9300 on-line consumers, three out of five consumers do not trust Web merchants (Jacobs, 1997). To combat this fear, consultants frequently advise e-commerce Web designers to include stated and authenticated policies of security (e.g. encryption and use of seals of approval) to communicate trustworthiness to the electronic consumer (Glass, 1998).

Most of the studies examining the impact of Web features on consumer trust and purchasing behavior rely on two primary kinds of evidence: consumers' retrospective reports (Jacobs, 1997; Muysken, 1998) and views of experts (Glass, 1998). Relying on consumer retrospective reports may introduce confounds such as purchasing histories and the nature of the established relationship with the marketer. Purchasing histories will introduce biases of product or brand preferences, while the use of current customers ignores the impact of the nature (impersonal or personalized) and stage (i.e. attraction, maintenance, etc.) of the trust building relationship (Cheskin and SA, 1999; Dayal et al., 1999). The present study uses an experimental design to investigate trust in business-to-consumer (B2C) e-commerce.

Three research questions guided this research:

1. What is the role of four commonly used Web privacy and security attributes in evoking consumer willingness to purchase online?

2. What role does trustworthiness play in a consumer's interaction with Web merchants?
3. What role does web design have in the consumer purchase decision?

Before addressing these questions, this paper clarifies a few definitional ambiguities and briefly reviews the relevant literature. Particular attention is given to B2C e-commerce.

2. Literature review

There are several definitions of electronic commerce (e-commerce) that exist in the trade press and in the academic literature. For some, e-commerce includes all 'consumer-oriented storefronts, business-to-business applications as well as behind-the-scenes business functions like electronic payment systems and order management' (Conhaim, 1998; p. 13). Different categorizations of electronic commerce exist, including business-to-consumer, business-to-business, and government-to-constituents. Business-to-consumer (B2C) e-commerce is defined as business transactions conducted between corporations and individual consumers. This is often represented as corporations' Web sites used to sell goods and services directly to consumers. Business-to-business (B2B) e-commerce is defined as transactions conducted electronically between organizations. Government-to-constituents (G2C) e-commerce defines the electronic relationship between the governments and various constituents including businesses, individuals, employees and other government agencies. This study focuses on B2C e-commerce as defined above.

Although business-to-consumer electronic commerce has experienced explosive growth, it is interesting to note that it still only accounts for a very small portion of overall consumer spending. Average spending online per customer in 1999 was $215. In 2000, it was $290 (Francis, 2000). Online retail sales in 1999 were close to U.S. $26.7 billion, and in 2000, they grew 66% to U.S. $44.5 billion. It is expected that by 2003, there will be 101.3 million buyers online in the United Sates only. However, despite this growth, in 2000, Internet-based retail sales represented only 1.7% of total retail sales, up from 1.1% in 1999, and were expected to reach only 2.5% in 2001 (Wingfield, 2001), indicating that there is significant potential for business-to-consumer electronic commerce to grow. For B2C e-commerce to reach its full potential, factors that may inhibit or facilitate the growth of the market must be better understood. One of these factors might be trust, as exemplified by the Organization for Economic Development (OECD)'s statement that trust is one of the critical themes for electronic commerce to grow.

2.1. Privacy and security

The promotion and optimum use of security, privacy and trustworthiness are important elements for supporting the growth of business-to-consumer e-commerce. Two problems with existing e-commerce literature include the extent to which privacy and security issues are conceptualized as distinct, and the lack of understanding of how they are related. As illustrated in the 2001, Harris Interactive poll discussed below, concerns about the safe

storage of information are mixed with sharing of information under the category of 'privacy' concerns. Another common practice in the literature is to use global terms such as safeguard assurances to represent both privacy and security concerns. This conceptual confusion is often followed by discussions of which type (privacy and/or security) of Web features maximally reduce consumer fears, in addition to how to place and convey these features on the site (Dayal et al., 1999; Woodlock, 1999/2000). As such, it is unknown whether consumers really see these as distinct issues. This study uses privacy and security as two clearly distinct constructs, which are defined below.

2.1.1. Privacy

It is the willingness of consumers to share information over the Internet that allows purchases to be concluded. However, it is clear that consumer concern with privacy of information is having an impact on the consumer Internet market, and that for electronic commerce to reach its full potential, this concern still needs to be addressed. For example, a Business Week/Harris poll of 999 consumers in 1998, revealed that privacy was the biggest obstacle preventing them from using Websites, above the issues of cost, ease of use, and unsolicited marketing (Green et al., 1998). In an IBM Multi-National Consumer Privacy Survey in 1999, 80% of the U.S. respondents felt that they had "lost all control over how personal information is collected and used by companies." Seventy-eight percent had refused to give information because they thought it was inappropriate in the circumstance, and 54% had decided not to purchase a product because of a concern over the use of their information collected in the transaction. Specifically, 72% of U.S. respondents were worried about the collection of information over the Internet. Another study by Forrester Research supports these findings, showing that two-thirds of consumers are worried about protecting personal information on-line (Branscum, 2000). The 2000 Pew Internet and American Life Survey reported that 66% of respondents believed that online tracking should be outlawed, and 81% supported rules for online information gathering. An impressive 86% believed that businesses should ask before collecting information about them (opt-in). And, in a 2000 National Consumers League survey, respondents ranked personal privacy above health care, education, crime and taxes as concerns (Paul, 2001). A 2001 survey by 'Harris Interactive for The Privacy Leadership Initiative' continued to document consumer concerns about protecting their privacy on the Internet, as individuals who have not bought over the Internet list security of information storage and transmission and the use of personal information as the top reasons why they have not purchased (Harris, 2001a). Fears of privacy violations were also documented in 2001 by an American Demographics survey, which listed children's privacy breaches as the most feared, followed by misuse of private information, financial theft, and identity theft (Paul, 2001).

Privacy issues on the Internet include 'spam', usage tracking and data collection, choice, and the sharing of information with third parties. These areas of concern are found in the taxonomy described by Wang et al. (1998), and are reflected in the Federal Trade Commission's standard for privacy on the Internet. The FTC identifies notice, choice, access and security as elements of a desirable privacy policy.

Consumers' reassurance that the information shared will be subjected to personally delineated limits is the essence of privacy on the Internet. Prior literature that recognizes

the importance of controlling information includes Hoffman et al. (1999) who identify the significance of 'control over secondary use of information' concerns by consumers involved in Internet transactions. Control over secondary use of information relates to the consumer's concern that once the information is freely submitted to a Web site, there is diminished or nonexistent control of the further sharing of that information with third parties. Consequently, for this research the definition of privacy that is adopted is *the ability to manage information about oneself.*

2.1.2. Security

A security threat has been defined as a "circumstance, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse" (Kalakota and Whinston, 1996). Security, then, is the protection against these threats. Under this definition, threats can be made either through network and data transaction attacks, or through unauthorized access by means of false or defective authentication. This definition must be tailored in order to be applicable to consumer transactions to acknowledge that consumer information has value. For consumers, it must be recognized that (1) economic hardship encompasses damages to privacy (loss of information) as well as theft, for example, of credit information and (2) authentication issues for consumers will be reversed; as in whether the Web site is 'real' rather than whether the purchaser's identity is real. This tailored definition explains the security threats from a consumer's standpoint. Security in B2C electronic commerce is reflected in the technologies used to protect and secure consumer data. Security concerns of consumers may be addressed by many of the same technology protections as those of businesses, such as encryption and authentication.[3] For purposes of this research, the application of specific security technologies is categorized as security features.

Our delineation of privacy and security is similar to the distinction that Hoffman et al. (1999) use in identifying 'environmental control' as separate from 'control over secondary use of information', described above. Environmental control refers to consumer concerns with sharing information online due to expectations of threats to online security, including fear of hackers and informational theft.

2.1.3. Privacy and security statements and third party verification

Privacy and security commitments in B2C e-commerce are reflected in the actions of the Web merchant. Yet, for consumers, the primary, visible access to privacy and security on Web merchants' sites is through statements that describe in more or less understandable terms the privacy and security policies of the Web merchant, from

[3] Encryption is the application of a mathematical algorithm to a message in order to scramble that message. The recipient must have the decrypting key to unscramble the message. Secure socket layer (SSL) technology is present in most modern Internet browsers, and encrypts information so that it is difficult to view the information without the authorized key. Secure electronic transaction (SET) is another encryption technology that additionally uses a certificate authority to apply the key for decryption and protects credit information by allowing only the payment clearinghouse, not the merchant, to view such information. The use of these technologies greatly decreases the opportunity for unauthorized access to information passed over the Internet.

information collected to data sharing policies, and security features such as encryption and password protections. The privacy and security statements on today's Web sites vary from excellent and well-detailed to hard to find and difficult to read.

Groups like TRUSTe or BBBOnLine offer programs that businesses can participate in to show their commitment to privacy or security. For example, TRUSTe states to consumers; "When you see the TRUSTe seal, you can be assured that you have full control over the uses of your personal information to protect your privacy." Once joining the program, the business is allowed to post the third-party privacy 'seal' indicating their participation. Third party security seals are increasingly used by businesses to communicate their commitment to security (e.g. Verisign).

The effectiveness of communicating privacy and security commitments to consumers by the use of third party verification programs would be important for electronic businesses to know. In a 2001 study, Harris reported that when consumers notice privacy seals they consider them important, and are more willing to provide personal information to the site because of the third party verification (Harris, 2001b). Another study reports that 60% of consumers indicated that privacy statements on Web sites made them feel more confident that the business would not misuse their information (Pastore, 2001). Recently, a survey conducted for Privacy and American Business found that 91% of consumers would feel more comfortable using sites participating in a third party verification program, and 84% believed that they should be required for electronic businesses. Furthermore, 62% believed that third party privacy seals would reduce their privacy concerns (Newsbytes, 2002).

Previous studies have found no negative correlation between the presence of privacy and security statements and the perceived risk of a site (Miyazaki and Fernandez, 2000). Yet, privacy and security statements of categories of Web sites do show a positive correlation with consumers' likelihood to purchase from those categories of sites (Miyazaki and Fernandez, 2000). A later study provided support for the relationship between security concerns and a consumer's willingness to purchase online, but did not support a relationship between privacy concerns and the willingness to purchase online (Miyazaki and Fernandez, 2001). Adding to this complex relationship is the fact that privacy and security seals may not be well recognized by consumers. Cheskin and SA (1999) found that even experienced Web users are less familiar with privacy and security seals than with the underlying concepts and technology that sites employ, such as cookies and encryption. Only 25% of consumers seem to recognize seal features on Web sites (Harris, 2001b).

As discussed above, prior research establishes that both privacy and security are important to the consumer. This prior research surrounding privacy and security sought to measure the importance of site attributes relating to privacy and security, not their relative importance. This research seeks to compare the relative importance of each of these areas, privacy and security seals and statements, and security features. While security features do not guarantee privacy and security, without features such as encrypted communications privacy and security are almost impossible to achieve. It is the premise of the first hypothesis that consumers will recognize that security features are the precursor to privacy and security.

Hypothesis 1. Consumers will rank security features as more important than security seals, privacy statements, and privacy seals in considering acquisitions of goods or services over the Web.

2.1.4. Trust and trustworthiness

People make important buying decisions based, in part, on their level of trust in the product, salesperson, and/or the company (Hosmer, 1995). Similarly, Internet shopping decisions involve trust not simply between the Internet merchant and the consumer, but also between the consumer and the computer system through which transactions are executed (Lee and Turban, 2001).

Although many studies have identified the critical role of consumer trust in Internet shopping, two critical issues have hampered empirical investigations of the impact of consumer trust on on-line purchasing activities. The first issue is centered on the lack of agreement about the definition of online consumer trust (Lee and Turban, 2001). Although most of these definitions capture the notion of risk taking, many are merely operationalizations taken from the traditional marketing literature and applied to the online context. More importantly, few of these definitions specify the on-line trust referents (i.e. the merchant or the computer system). For example, Moorman et al. (1993, p. 82) define consumer trust as "a willingness to rely on an exchange partner in whom one has confidence'. This definition suggests that trust reflects a continuum of readiness (i.e. readiness to engage in a relationship with the other party, such as a salesperson) (Crosby et al., 1990). Rather than focusing on trust in individuals, this study focuses on the electronic organization as well as its site as the exchange party.

The second issue hampering richer examinations of Internet consumer trust is the lack of empirical attention given to one critical antecedent of consumer trust: perceived trustworthiness (Lee and Turban, 2001). Several researchers have identified and validated three main elements of trustworthiness: *ability*, *benevolence*, and *integrity* (Mayer et al., 1995; Lee and Turban, 2001). According to these scholars, the ability of a merchant is reflected in its ability to handle sales transactions and the expertise to generally conduct business over the Internet. In contrast, perceived integrity is evidence of the marketer's honesty and sincerity. Finally, benevolence was defined as the extent to which the trusting party believes that the trusted party wants to do good things rather than just maximize profit. In contrast to the other two transaction focused dimensions, benevolence reflects perceptions of the marketer's willingness to engage in discretionary or philanthropic commitment to its customers. A similar dimensional distinction can be found in the corporate social responsibility literature (Carroll, 1979; Smith et al., 2001). According to this literature, stakeholders such as consumers, employees, board members value merchant characteristics (such as transaction abilities, legal integrity, and ethical orientation) significantly more than the merchant's discretionary or philanthropic responsibilities (Edmondson and Carroll, 1999; Ibrahim and Angelids, 1993). Additional insights from this literature also indicate that a firm's economic responsibilities (make a profit) and its discretionary responsibilities are often negatively correlated (Ibrahim et al., 1997). These findings suggest that consumers expect marketers to be competent (have high ability) primarily focus on maximizing profits often at the cost of being benevolent. While

this study will focus only on ability (also known as reliability) and integrity indices of trustworthiness, we believe future studies should include the relative impact of the benevolence dimension consumer behavior.

For purposes of this research, *trustworthiness* is defined as the *perception of confidence in the electronic marketer's reliability and integrity*. This definition highlights the need for e-commerce firms to reliably protect (secure) the private information given by customers and to use it with integrity in order to increase electronic consumer trust. This definition will facilitate the examination of the nature of the relationships among trustworthiness, privacy, security, and purchase intentions.

2.1.5. Factors influencing perceptions of trustworthiness

Online marketers may elect to influence perceptions of trustworthiness by using a variety of strategies. For instance, the use of the TRUSTe symbol, the CPA WebTrust, and the activities of the Online Better Business Bureau are examples of private activities designed to build trustworthy images. Similarly, WebTrust Privacy seal programs may engender perceptions of trustworthiness when considering its auditing requirements.

Consumers often make important buying decisions based, in part, on their level of trust in the product, salesperson, and/or the company (Hosmer, 1995). Internet shopping decisions, however, involve trust not simply between the Internet merchant and the consumer, but also between the consumer and the computer system through which transactions are executed (Lee and Turban, 2001). For example, one of the factors influencing trustworthiness identified by Singh and Sirdeshmukh (2000) is technical competence, as measured by the technical ability of the Web merchant to conduct the e-commerce transactions correctly (Cheung and Lee, 2001; Ratnasingham and Kumar, 2000). So, while privacy and security strategies are commonly used, online marketers may also build perceptions of trustworthiness by designing effective customer interfaces. Like physical store customers, electronic customers tend to trust marketers that provide continuous service. Online marketers may convey their commitment to continuous service with the inclusion of customer service links, interactive email, and a help button on their Web site (Lohse and Spiller, 1998). Similarly, a marketer's integrity can be inferred from explicit information about shipping and handling costs, guarantees, and statements about product quality.

Given the critical role of the above transaction practices in building perceptions of trustworthiness, trust indices may explain very little variance in assessments of the marketer's trustworthiness. In fact, given the common lack of familiarity with the above trust indices, the second hypothesis proposes that there may exist a negative relationship between perceptions of trustworthiness and the presence of trust indices.

Hypothesis 2. The consumer's perceptions of a marketer's trustworthiness may be high even when trust indices (seals and statements of privacy and security) are weak.

2.1.6. Entity type

According to Papadopoulou et al. (2001), trust is an essential prerequisite for electronic customer relationship building. A notable characteristic of electronic relationships is

the need to exchange personal information beyond that required to complete a traditional transaction. Under what circumstances customers are willing to provide personal information is still unknown. For example, when intending to purchase from an online marketer, will customers provide private information regardless of the marketer's perceived trustworthiness? The answer to this question will likely depend on a variety of factors in the e-commerce context. This paper examines the impact of the type of entity or marketer (i.e. electronic-only or land and electronic) on the relationship between the consumers' willingness to provide private information and their purchase intentions. Electronic-only merchants are those with no physical stores. Land and electronic merchants have both physical stores and electronic storefronts.

Consumer perceptions of trustworthiness may be less important in the purchasing decision when deciding to purchase from a land and electronic Web marketer. Studies have shown that face-to-face interactions evoke higher levels of trust (Cassell and Bickmore, 2000). As such, it can be expected that higher levels of trust would emerge in exchange relationships where the consumer has the possibility of physical access to the online marketer. Being able to return items to a marketer with ease is both convenient and assuring. Thus, purchases from land and electronic marketers will likely be perceived as less risky purchases, regardless of the perceptions of the marketers' trustworthiness from the Web site.

In contrast, electronic-only sites do not have such assurances. As a result, it can be expected that assessments of the marketer's trustworthiness may be much more important when transacting with an electronic-only marketer. Under these circumstances, it seems likely that removing the linear effects of trustworthiness would result in the absence of (or, at best, a spurious) relationship between purchase intentions and consumer readiness to give personal information. In essence, perceptions of trustworthiness may be essential when initiating a transaction with an electronic-only marketer since without trust, no private information will be given, and no sale will be initiated.

Hypothesis 3a. When controlling for trustworthiness perceptions, there will be a positive relationship between the consumers' purchase intentions and their willingness to give private information to a land and electronic merchant.

Hypothesis 3b. When controlling for trustworthiness perceptions, there will be no significant relationship between the consumers' purchase intentions and their willingness to give private information to an electronic-only marketer.

2.1.7. Design features

Research focusing on creating a pleasurable online experience has focused on Web site attributes that quiet the fears of consumers and produce a satisfying and enjoyable experience for the consumer. Web interface design issues such as convenience, personalization capabilities, and ease of use are the focus of this literature (Lohse and Spiller, 1998). Sacharow (1998) combines these two perspectives and defines consumer online comfort as a balance between letting the personalization capabilities of the Internet give consumers what they want, while simultaneously giving them control over who has

access to their private information. One survey indicated that attributes that contribute to convenience and are cosmetically pleasing affect the consumer's online actions (Cheskin and SA, 1999). These features may lead to increased willingness to trust or to purchase from a Web site.

The fourth hypothesis of this research seeks to extend the research by examining the comparative significance of privacy and security features to design features in the online consumer's willingness to purchase. Under what conditions does the consumer rank 'pleasure' features more important than 'trust' features (including security and privacy features) when assessing an intention to purchase? No studies to date empirically tested this assertion. This study takes an initial step in that direction. Because previous research has compared these attributes only separately, without studying any intertwining relationship, it is difficult to predict which would be most important to the consumer. However, it is the hypothesis of this research that the convenience and ease of use features will be more important to consumers. Security and privacy are complex, and the indices of these are often difficult to determine. Whether a web site is easy to use is a straightforward and easier determination. In addition, intuitively privacy and security of the online experience is not why consumers would go to the Internet to purchase in the first place—the convenience of buying online may be the primary reason that a purchaser goes online to purchase. Thus, the fourth hypothesis suggests that the convenience, pleasure factors may be more important in the decision to purchase online when compared to privacy and security features.

Hypothesis 4. Consumers will report that privacy and security features are less important than pleasure features (convenience, ease of use, cosmetics) to their intention to purchase.

2.2. Research model

Building upon the above discussion and hypotheses, a research model depicting the constructs and relationships examined in this study is depicted in Fig. 1. As a descriptive framework, the model does not illustrate each hypothesis with a specific linkage, but provides a means to organize the primary constructs in this study. For example, at a macro-level, the Web feature grouping includes categories of privacy, security, and pleasure site attributes. The privacy category consists of privacy statements and third party privacy seals. Similarly, features in the security category include third party security seals and security features commonly found on Web sites (encryption and password protections). The relative importance of these features and their relationship to the consumer's perceptions of a marketer's trustworthiness are tested in Hypotheses 1 and 2.

How the marketer's origin (i.e. land or electronic) may be related to the consumers' purchase intentions and their willingness to give private information is tested in Hypotheses 3a and 3b. Finally, the study examines the extent to which consumers rank pleasure features (convenience, ease of use, attractiveness) more important than privacy and security features (Hypothesis 4).

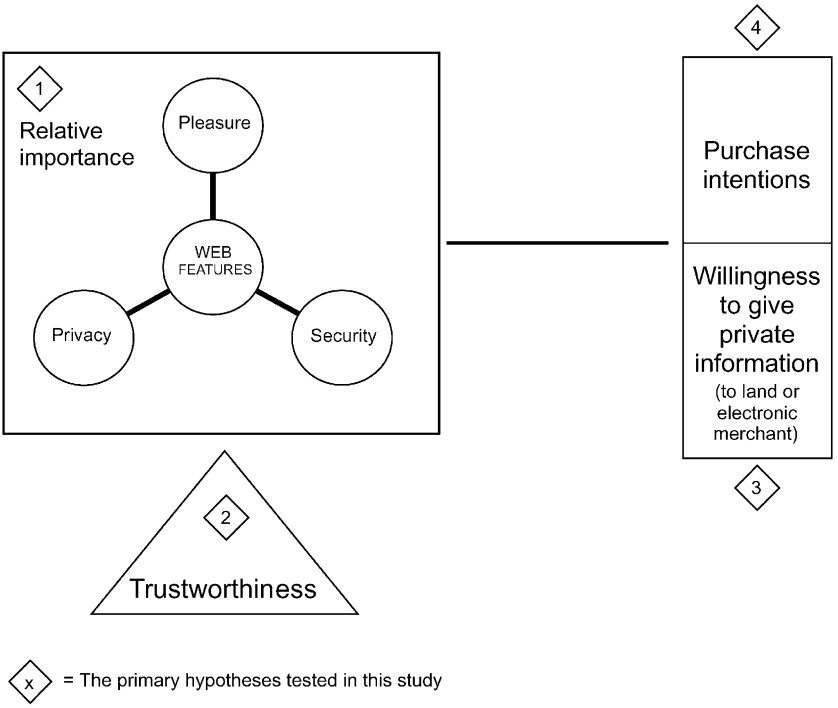

Fig. 1. Descriptive organizing framework of research constructs.

3. Methodology

3.1. Sample

One hundred and forty U.S. southeastern university students volunteered to participate in the study and received extra credit for doing so. Fifty percent of the subjects were females, and all subjects ranged in ages between 19 and 26 years old. The profile of these students is consistent with the findings of YouthStream Media Networks and Greenfield (2000). This sample had access to the Internet from a variety of locations, and the majority had made an online purchase prior to the study. Table 1 shows demographics for the sample.

3.2. Procedures

Two researchers identified a variety of e-commerce Web sites to be included in the study. Multiple sites were reviewed, and four were selected. The chosen sites reflected a combination of privacy and security features, seals, and statements. The four sites included two electronic-only businesses and two land and electronic businesses. The two land and electronic sites included companies who are not primarily catalog retailers. The four Web sites' addresses were saved on a system that randomized the order in which they were presented. Participants were randomly seated at computer

Table 1
Demographics

	Females	Males	Total
n	70	70	140
Average age	20.5	21.5	21
Access to computer	70 (100%)	70 (100%)	140 (100%)
Access to credit card	66 (94%)	67 (96%)	133 (95%)
Work experience			
0–2 years	16	21	37
2–4 years	23	25	48
4–8 years	27	23	50
>8 years	4	1	5
Average number of prior Web purchases in last 3 years	13	12	13

workstations. Instructions were provided online on the initial screen that was presented to participants as they sat at their assigned station. Participants were asked to answer the pre-study survey, and then were instructed to visit Web sites where purchasing decisions could be made. Participants could navigate further into the sites once they were presented with the initial homepages. Final instructions were given on the post-study survey and end of session procedures.

After being seated at their workstations, subjects were given a packet of research materials. In this packet were: (a) one general beliefs questionnaire, (b) four survey sheets designed to measure consumer reactions to each site, and (c) one post-study personal data sheet. The total time elapsed between the first session and last session, including the time that was used by experts to rank security and privacy features (described below) was 1 week. This ensured that everyone viewed the same information when evaluating the Web sites.

3.3. Measures

3.3.1. Overview

The survey sheets distributed in this study asked participants to 'assume they were interested in purchasing the products or services offered by this marketer.' They were then asked to indicate how much they agreed to statements about the site. A seven-point Likert type scale ranging from strongly disagree (1) to strongly agree (7) was used. The questions focused on the respondents' intentions to purchase, willingness to provide information about themselves, site quality, and the trustworthiness of this marketer. The source and nature of these scales are discussed below. All participants rated every Web site.

3.3.2. Trustworthiness

This 3-item scale was tested by Lynch et al. (2001) on two samples, reporting Cronbach's alpha of 0.86 and 0.84, respectively.

3.3.3. Site quality

The scale measuring the perceived quality (pleasure features) of the Web site was comprised of items adapted from a scale developed by Lynch et al. (2001) and items developed by the authors. In his research, Lynch et al. (2001) reported reliability estimates across two samples for the original 4-item scale. They were 0.78 and 0.85, respectively. Based on a review of the literature, one additional item was added by the authors.

3.3.4. Intentions to purchase

Intention to purchase from a Web site was measured using a scale developed by Gefen (2000). This 4-item scale measured both inquiry and buying intentions. The reported reliability of the scale was 0.81.

3.3.5. Privacy and security features

As noted in the literature review, privacy and security features have been investigated by numerous researchers. From this literature, four types of privacy and security features were identified and incorporated into the study. These four features were (1) third party privacy seal, (2) third party security seal, (3) security features, and (4) privacy statements. To be in line with the other items in this study, these four features were placed in questions, so that the response categories were all based on the level of importance (1–5) to "How important are ___ in your decision to buy on the World Wide Web?"

3.3.6. Demographics

Respondents were asked to indicate their race, gender, experience with Internet purchasing, and access to computers and credit cards.

3.3.7. Expert ratings

Two experts were asked to rate every Web site for the strength of its privacy and security policies. The use of multiple raters is highly recommended by researchers. Both experts are academicians active in conducting research and publishing in the area of electronic commerce, with special focus on cyberlaw and privacy, and security and e-commerce adoption. One expert was a member of the research team, while the second expert was external to the research team and not involved in this study.

3.4. Instrument validation

Before using the collected data for hypothesis testing, the instrument was subjected to reliability and validity analyses. Reliability was assessed using Cronbach's alpha, while validity was assessed using factor analysis.

3.4.1. Reliability

The scales used in the study exhibited reliability levels in the accepted range. Table 2 presents the reliability estimates across the four sites used in the study. For trustworthiness, the average reliability estimate of the scale across all four sites was 0.80. Perceptions of the Amazon.com site were more consistent ($\alpha = 0.88$) than those of the Smart Bargains' site ($\alpha = 0.74$). Nevertheless, the reliabilities were consistent with

Table 2
Site reliability coefficients

Scale	Number of items	Amazon	Foot Locker	Athlete's Foot	Smart bargains	Average
Site quality	4	0.55	0.80	0.80	0.72	0.72
Purchase intentions	3	0.89	0.80	0.77	0.80	0.82
Site trustworthiness	3	0.88	0.78	0.80	0.74	0.80
Importance of security and privacy features	4	Na	Na	Na	Na	0.86

prior results (0.84 and 0.86). For site quality, the modified scale originally exhibited low reliability, mostly due to one unreliable item (SQUAL3), which was dropped from further analysis. The Cronbach's alpha for this modified scale varied widely across the sites, ranging from 0.55 to 0.80; however, the average reliability coefficient for this scale was 0.72, slightly under previous studies' results (0.78 and 0.85), but still acceptable. The intentions to purchase scale exhibited reliability estimates slightly above that reported by Gefen (2000) at $\alpha = 0.82$. Finally, the privacy and security features scales, created by the authors, had an internal validity coefficient of 0.86. The final reliability estimates, means, and correlations are shown in Table 3.

3.4.2. Factor analysis

Unidimensionality of the scales was evaluated using factor analysis. The analysis used a principal components extraction method with promax rotation. The promax rotation was used because it is an oblique rotation method, which allows for correlated factors. Since it is likely that perceptions are correlated with one another, an oblique rotation is appropriate. Results of these analyses are presented in Table 4. When testing for the instrument's validity using the collected data, four factors emerged. This is consistent with the instrument's underlying structure, and reflects the factors identified from the previous literature.

Table 3
Means, standard deviations, average reliability coefficients and correlations

		n	Number of items	Scale mean	Std dev	α	1	2	3
1	Site Quality	140	4	5.51	0.60	0.72			
2	Intentions towards purchase	140	3	4.59	0.97	0.82	0.61**		
3	Site Trustworthiness	140	3	5.06	0.63	0.80	0.64**	0.61**	
4	Importance of privacy and security features	140	4	3.69	0.85	0.86	−0.02	−0.21*	−0.05

*$p < 0.05$; **$p < 0.01$.

Table 4
Factor analysis

Variable	Description	Importance of features	Site quality	Purchase intention	Site trustworthiness
IMPORT1	How important are security FEATURES (e.g. SET, SSL, locks, etc.) in your decision to buy on the World Wide Web?	0.81			
IMPORT2	How important are third party PRIVACY SEALS in your decision to buy on the World Wide Web?	0.87			
IMPORT3	How important is the content of the privacy policy statement in your decision to purchase on the World Wide Web?	0.79			
IMPORT4	How important are third party SECURITY SEALS in your decision to buy on the World Wide Web?	0.88			
SQUAL1	This web site was easy to use		0.81		
SQUAL2	This web site had helpful pictures and graphics		0.78		
SQUAL3	This web site provided complete information		0.59		
SQUAL4	I would give this web site an excellent rating		0.61		
INTENT1	I am very likely to buy from this web site			0.96	
INTENT2	I would create a personalized account at this site			0.78	
INTENT3	I would use my credit card to purchase from this web site			0.66	
TRUST1	This web site is trustworthy				0.87
TRUST2	This web site will keep its promises and commitments				0.69
TRUST3	This web site has a good reputation				0.77

3.4.3. Expert ratings

The expert ratings for privacy and security features were subjected to validity analyses using the inter-rater agreement measure called Cohen's Kappa *(k)*. This metric of the strength of agreement between two raters measures the 'proportion of agreement between two groups adjusted for agreement attributable to chance' (Reynolds, 1977; p. 59). Levels of agreement above zero indicate some agreement not attributable to chance (e.g. when $k > 0$ there is more agreement between raters than can be expected by chance). k is defined as follows:

$$k = \frac{\sum f_{ii} - 1/n \sum f_{i+} f_{+i}}{n - 1/n \sum f_{i+} f_{+i}}$$

where $\sum f_{i+} f_{+i}$ and $\sum f_{i+} f_{+i}$ represent sums of diagonal and off-diagonal elements of the agreement matrix. Using Cohen's Kappa as a measure of agreement instead of simple correlation provides the researcher with greater confidence in the ratings obtained. As can be

Table 5
Expert ratings-privacy

Site	Score component	Rating (expert)		Composite score[a]	Inter-rater reliability[b]
		1	2		
Amazon	Presence of privacy statement	Y	Y	2.17	1.00
	Accessibility of privacy statement	W	W		
	Content of privacy statement	W	W		
	Presence of privacy seal	N	N		
Athlete's foot	Presence of privacy statement	Y	Y	3.67	0.33
	Accessibility of privacy statement	M	S		
	Content of privacy statement	S	M		
	Presence of privacy seal	Y	Y		
Foot locker	Presence of privacy statement	Y	Y	3.33	0.64
	Accessibility of privacy statement	S	M		
	Content of privacy statement	S	S		
	Presence of privacy seal	N	N		
Smart bargains	Presence of privacy statement	Y	Y	3.00	1.00
	Accessibility of privacy statement	W	W		
	Content of privacy statement	M	M		
	Presence of privacy seal	Y	Y		

[a] The composite score was obtained by first assigning values of 1 or 2 for no or yes, 1, 2, or 3 for weak, medium or strong, respectively. The ratings were then standardized and finally aggregated into a standardized composite score for each Web site and each expert, and then scores of each expert were averaged to obtain the final composite score. Amazon example: $2/2 + 1/3 + 1/3 + 1/2 = 2.17 \times 2/2$. These scores do not represent 'absolute' values of strengths/weaknesses, but rather relative strengths between sites.
[b] Cohen's Kappa.

seen from Tables 5 and 6, substantial agreement was achieved between the two experts on numerous sites for both security and privacy indices.

While the two low scores of 0.33 and 0.43 might seem to show low agreement, it must be remembered that Cohen's Kappa offers a much stronger evaluation of agreement because it measures agreement beyond what could be due to chance, something that simple correlations would not do. For rating schemes or classification of categorical data, Landis and Koch (1977) suggest the levels of strengths of agreement using Cohen's kappa measure as follows: less than 0.00 is poor; 0.00–0.20 is slight; 0.21–0.40 is fair; 0.41–0.60 is moderate; 0.61–0.80 is substantial; and 0.81–1.00 is almost perfect. Using this scheme, we have two 'perfect' scores, one (almost two) substantial agreement levels, and three moderate levels of agreement. Just one item has a 'fair' level of agreement (Athlete's Foot privacy rating). Given the acceptability of these agreement levels, the scores between the two raters were averaged to obtain final indices for security and privacy for each site. While the experts did not completely agree on the contents of their sub-ratings for Athlete's Foot privacy elements, they ended up with the same overall rating (3.67). As a result, even though the inter-rater agreement was not high, the results of the hypothesis test (for Hypothesis 2) were not affected. Athlete's Foot privacy rating by experts was, independently for both experts, the highest rating of all sites.

Table 6
Expert ratings-security

Site	Score component	Rating (expert)		Composite score[a]	Inter-rater reliability[b]
		1	2		
Amazon	Presence of security statement	Y	Y	2.17	0.50
	Accessibility of security statement	W	W		
	Content of security statement/Tools used	M	W		
	Presence of security seal	N	N		
Athlete's foot	Presence of security statement	Y	Y	3.08	0.60
	Accessibility of security statement	M	M		
	Content of security statement/Tools used	S	W		
	Presence of security seal	N	N		
Foot locker	Presence of security statement	Y	Y	3.42	0.56
	Accessibility of security statement	W	M		
	Content of security statement/Tools used	S	S		
	Presence of security seal	Y	Y		
Smart bargains	Presence of security statement	Y	Y	3.00	0.43
	Accessibility of security statement	M	M		
	Content of security statement/tools used	S	W		
	Presence of security seal	Y	Y		

[a] The composite score was obtained by first assigning values of 1 or 2 for no or yes, 1, 2, or 3 for weak, medium or strong, respectively. The ratings were then standardized, aggregated into a standardized composite score for each Web site and each expert, and then scores of each expert were averaged to obtain the final composite score.
[b] Cohen's Kappa.

4. Results

4.1. Indices of trustworthiness

Paired comparison *t*-tests yielded mixed results when testing our first hypothesis (*consumers will rank security features as more important than security seals*, *privacy statements*, *and privacy seals*). As expected, our respondents ranked security features higher than privacy statements, security seals and privacy seals. Privacy statements ranked significantly lower than security features ($t = 8.46$, $p < 0.001$). However, customers did not rank the third party security seals ($\mu = 3.57$) significantly higher than the privacy seals ($\mu = 3.56$). And, interestingly, the ranking of third party security seals ($\mu = 3.56$) was comparable in importance to both the privacy statements and third party privacy seals. These results are presented in Table 7.

As shown in Table 7, these site attributes were also significantly correlated, indicating that the desire for one is positively related to the others. One interpretation of these findings is that electronic consumers desiring statements of privacy are also likely to desire other indices of privacy and security.

Table 7
Means, standard deviations, and correlations for security and privacy features

	Rank	*n*	Mean	Std Dev	1	2	3
Security features (SET, SSL, locks, etc.)	1	140	4.15	0.9591			
Third Party Privacy Seals	2	140	3.57	1.0046	0.55**		
Third Party Security Seals	3	140	3.56	1.0676	0.59**	0.76**	
Privacy Policy Statements	4	140	3.49	1.0560	0.59**	0.54**	0.57**

**$p < 0.01$.

4.2. Indices of trustworthiness and consumer perceptions of trustworthiness

4.2.1. Trustworthiness ratings

To assess the average trustworthiness values allocated to each site by our respondents, mean responses were calculated. Using these means, mean score percentages were computed. These mean score percentages reflect the relative magnitude of the respondents' trustworthiness beliefs about each site. As can be seen in Table 8, our respondents believed the Amazon site was most trustworthy ($\mu = 5.62$), followed by the Foot Locker ($\mu = 5.32$), Athlete's Foot ($\mu = 4.85$), and Smart Bargains' ($\mu = 4.47$) sites.

Paired comparison *t*-tests were used to determine if the mean responses of the trustworthiness values were statistically different. For example, our respondents rated Amazon significantly higher in trustworthiness than Athlete's Foot ($t = 9.18$; $p < 0.001$), Foot Locker ($t = 3.61$; $p < 0.001$), or Smart Bargains ($t = 12.34$; $p < 0.001$). All other paired comparisons were statistically significant. The respondent rankings indicated in Table 8 were generated based on these statistical comparisons.

4.2.2. Experts' ratings

Our experts gave Amazon the lowest ratings on privacy and security features (2.17), while Smart Bargains earned a third place ranking (3.00). The first and second place rankings varied across the privacy and security conditions. When evaluating privacy features, Athlete's Foot earned the top rating (3.67) followed by Foot Locker (3.33). When evaluating the security features these two sites earned a reverse ranking from our experts.

Table 8
Expert vs. respondent ratings of trustworthiness, privacy, and security features

Site	Respondents' means scores	Respondents' ranking of trustworthiness	Experts' privacy ranking	Experts' security ranking
Amazon	5.62	1	4	4
Foot Locker	5.32	2	2	1
Athlete's Foot	4.85	3	1	2
Smart Bargains	4.47	4	3	3

In general, the trust indices of Athlete's Foot and Foot Locker were perceived to be more rigorous than those of Smart Bargains and Amazon.

To test Hypothesis 2 (*perceptions of a marketer's trustworthiness may be high even when trust indices* (*privacy and security features*) *are weak*), the trust indices ratings (provided by our experts) were contrasted with respondents' relative ranking of each site's perceived level of trustworthiness. A comparison of the relative order of the two rankings suggests that the hypothesis was partially supported. As can be seen in Table 8, in many cases, the experts' evaluation of the quality of the sites' trust indices was inversely related to the consumers' perceptions of trustworthiness. For example, Amazon was perceived as the most trustworthy by the respondents while the experts ranked its trust indices as least effective. In contrast, Athlete's Foot received lower ratings of perceived trustworthiness while the experts rank this site's privacy features as number one and its security features as number two in rigor. Consistent with the hypothesis, it seems likely that features other than trust indices (e.g. pleasure and transactive features) may be influencing perceptions of trustworthiness.

4.3. Importance of trustworthiness perceptions

To test Hypotheses 3a and 3b, partial correlations were generated and analyzed. Partial correlations provide the researcher with a single measure of association describing the relationship between two variables while adjusting for the effects of one or more additional variables. In essence, partial correlations allow the researcher to remove the effect of the control variable from the relationship between the independent and dependent variables. This is done based on the prediction that the control variable has some effect on both the independent and dependent variables. Testing Hypotheses 3a and 3b using partial correlations allowed the researchers to remove the linear effects of trustworthiness, in order to examine the spurious or genuine nature of the relationship between purchase intentions and consumer's ratings of the importance of privacy features.

To test these hypotheses, all marketers were classified into two categories: (a) land and electronic, and (b) electronic only. Amazon and Smart Bargains sites were classified as electronic only while Foot Locker and Athletes' Foot were categorized as land and electronic. Hypothesis 3a (*controlling for trustworthiness*, *consumers willingness to give private information will be positively related to their purchase intentions for land and electronic marketers*) was supported ($r_{\text{intent/willingness}} = 0.65$, $p < 0.000$). Hypothesis 3b, however, was not supported since consumers purchase intentions' relationship to their willingness to give private information was also significant ($r_{\text{intent/willingness}} = 0.64$, $p < 0.000$) for electronic-only merchants. These results suggest that trustworthiness is imperative in the decision to provide private information regardless of the type of marketer.

4.4. Web site features

Respondents were asked to evaluate site cosmetics and convenience features for each Web site. Research has shown that these features influence consumer willingness to make online purchases (Cheskin and SA, 1999). Since these attributes focus on creating a

Table 9
Hypothesis 4 regression results: purchase intentions

Variables	Coefficients	t	p	Adjusted R^2
(Constant)	4.75	0.07	0.942	0.40
Importance[a]	−0.23	−3.05	0.003	
Site quality	0.98	9.26	0.000	

[a] Importance: importance of privacy and security features.

satisfying and enjoyable experience for the customer, they have been described as pleasure attributes. Regression was used to test Hypothesis 4 (*consumers will report that privacy and security features are less important than pleasure features* (*convenience*, *ease of use*, *cosmetics*) *to their intention to purchase*).This hypothesis was supported (adjusted $R^2 = 0.40$) as shown in Table 9. It would appear that e-commerce is as much about convenience and aesthetics as in traditional markets. Surprisingly, privacy and security features were negatively related to purchase intentions. These results suggest that having a satisfying and pleasurable experience drives purchase intentions regardless of privacy and security concerns.

5. Discussion

This research examined the consequences of security, privacy, Web site attributes, and trustworthiness in business-to-consumer e-commerce. Table 10 summarizes the hypotheses and the results.

One of the study's primary goals was to examine the relative importance of site attributes reflecting security and privacy. The results indicate that the presence of security features was most important to the consumer. It is possible that recent terrorist attacks have intensified the consumer's desire for strong security. The presence of a privacy seal was least important to the sample. This finding is consistent with the results of a previous study where fewer than 14% of 2000 experienced users said they would trust a site that has a third party seal. The present research adds support to the researcher's conclusion that it seems these trust brands have some trust building of their own to do (Kuchinskas, 1999). Indeed, since later surveys have shown overwhelming support for the concept of third party verification, the findings of this research emphasize that the possible potential of seals has not been realized (Newsbytes, 2002). Although security features were ranked as most important by the sample, with privacy and security seals and privacy and security statements all highly correlated, respondents indicate that requirements for one of these features on a Web site lead to a desire for the others as well. Marketers who intend to include either strong privacy or security statements or features on their site should seriously consider including all of them. It is also possible that users generally understand the concept of security better than privacy because security is a more concrete concept. The notion of personal information and its control are rather nebulous concepts and may

Table 10
Summary of hypotheses and results

	Description	Analysis method	Result
H1	Consumers will rank security features as more important than security seals, privacy statements, and privacy seals in considering acquisitions of goods or services over the Web	Paired *t*-tests	Supported
H2	The consumer's perceptions of a marketer's trustworthiness may be high even when trust indices (seals and statements of privacy and security) are weak	Relative ranks	Not supported
H3a	Controlling for trustworthiness perceptions, there is a positive relationship between consumers' purchase intentions and their willingness to give private information to a land and electronic merchant	Partial correlations	Supported
H3b	Controlling for trustworthiness perceptions, there is no significant relationship between consumers' purchase intentions and their willingness to give private information to an electronic-only marketer	Partial correlations	Not supported
H4	Consumers will report that privacy and security features are less important than 'pleasure' features (convenience, ease of use, cosmetics) to their intention to purchase	Regression analysis	Supported

mean many different things to different folks. People tend to rate important what they understand. If students understood security better than privacy, then this understanding might influence their rankings. If this is true, educational and promotional efforts to explain privacy policies and seals might be well worth the marketers' time and effort so that these attributes address the previously documented concerns of consumers about their privacy. Privacy statements are not as simple to recognize as security features, and may not be as easily understood. Privacy statements are not always in favor of the consumer, while security features are consistent in their meaning. Efforts to make statements easily recognizable and effective may be worthwhile.

In this paper, trustworthiness was defined as the perception of confidence in the electronic marketer's reliability and integrity. The second hypothesis tested the relationship between privacy and security statements and seals on perceived trustworthiness. It was not supported. While trust indices appear to be important to consumers, the results suggest that the quality and salience of these expressions of privacy and security may not drive conclusions about the trustworthiness of a marketer. A closer look at the data indicates that for one of the sites (Amazon) perceptions of a marketer's trustworthiness was high even when privacy and security features were weak. This finding is important to marketers in that it suggests that the prominent display of trust indices is an important practice but alone the indices do not engender high trustworthiness perceptions. For example, the marketer's reputation, cosmetics, and other Web attributes can lead to higher perceptions of trust even when

weak trust indices are present on the Web site. The above finding suggests that certain levels of reliability and integrity are necessary, but they are not sufficient above some unknown threshold. Another possible explanation for this result is that the respondents may have lacked familiarity with or understanding of the seals and statements. This hypothesis warrants further study.

Another goal of this paper was to explore the nature of the relationship between the decision to provide private information and purchase intentions when controlling for trustworthiness (H3). The results suggest that the marketer's trustworthiness drives the decision to provide personal information, regardless of the type of marketer. Previous research has suggested that the importance of trustworthiness in the purchasing decision may depend on situational factors. For example, in the traditional marketing literature, Garbarino and Johnson (1999) found that for low relational customers (e.g. individual ticket buyers and occasional subscribers), trustworthiness is not a primary mediating construct between attitudes and purchase intentions. In contrast, for high relational customers (e.g. on-going subscribers) it is essential. Two additional situational factors in the e-commerce exchange relationship were examined in this study: the type of marketer and the level of trustworthiness. Further research is warranted to explore this relationship.

A final goal of the study was to further evaluate the relative effects of site quality and perceived trustworthiness of the Web site on purchase intentions (H4). The results indicate that both constructs are significantly related to purchase intentions. However, the importance of security and privacy features has a negative relationship with purchase intentions, while the quality of the site has a positive relationship with purchase intentions. In light of many surveys and reports of the importance of privacy and security to consumers' decision to purchase on Web sites, a possible interpretation of this result is that those consumers who intend to purchase have already resolved any discomfort or distrust based on privacy and security concerns. Alternatively, the results may show that although consumers may express a desire for privacy and security, when the decision to purchase is actually made, they do not operationalize these preferences. Similar to the decision to fly on a commercial airline, prominent indices of safety and privacy are necessary, but the primary factors driving a passenger's decision to fly is convenience, cosmetics, and cost. Prominent trust indices may be considered 'white noise' and may be viewed as impediments to convenience priorities.

5.1. Contributions

The present research provides several preliminary insights into the role of trustworthiness, security, privacy and other Web site attributes in e-commerce. For practitioners, the results suggest that security is highly valued by consumers. The findings provide further support for the importance of Web site attributes (reputation and convenience) above and beyond privacy and security concerns. For example, the addition of shopping carts and easy checkouts (or express checkouts) can improve the convenience of shopping on a Web merchant's site, and ultimately improve repeat sales (Cheskin and SA, 1999). One additional finding that has implications for practitioners is that trustworthiness of the Web merchant is important irrespective of

whether the merchant is a land and electronic or electronic only merchant. All merchants should therefore develop strategies to increase consumers perceptions of their trustworthiness.

For researchers, this preliminary research provides some interesting questions and a base model to explore the roles of trustworthiness, privacy and security in electronic commerce further. The study also highlights the importance of using security and privacy as two distinct concepts, even though they are conceptually related.

Several limitations inherent in the design of the present study provide for future research opportunities. First, although a desirable benefit of an experimental design is the ability to isolate particular variables of interest and test for predicted effects, a weakness of such design is its inability to truly capture other dynamic processes at work within a complex business environment. Toward this end, after theoretically driven research models have been developed and tested, future research should employ other methods in order to provide a triangulation with the present findings. It is suggested that a survey and interview approach that targets both experienced and non-experienced potential consumers should be undertaken. An important outcome of such a research strategy should be the ability to contrast the attitudes, motivations, and intentions of experienced and less experienced consumers by the nature of the desired e-commerce relationship (high versus low relational customers).

Another potential limitation to the study is due to the fact that respondents were asked to assume they were interested in purchasing from the Web sites before answering the survey questions, but were not actually given money to purchase anything. As a result, external factors such as their lack of interest in the Web site's products or their positive or negative prior experience with the Web site might have affected the results. The choice of Web sites, however, may have helped alleviate part of this potential concern, since all of the sites offered products typically of interest to the sample's consumer group (sportswear, sport footwear, books, and bargain items).

An issue often raised by researchers is whether the use of students for a study limits the validity of the results obtained. Some may feel that the students' perceptions are different than those of the general population. While this may be true, two factors minimize this issue. First, recent research shows that the belief that perceptions of students and general consumers are different may not be always valid. For example, in a recent study of Indian consumers it was determined that there are no statistically significant differences between students' and general consumers' beliefs and attitudes toward advertising (Durvasula et al., 1997). Second, it should be noted that several early surveys of Internet users reveal that young people with above average education form the majority of users; therefore, they also form the majority of potential Web buyers. While using student subjects to evaluate managerial decision-making processes might wrongly represent the intended population, asking students to answer questions as potential Web consumers is asking them to be in a potential real life situation for them.

In addition, research relying on experts can be expected to affect the external validity of the findings. Since the expansion of B2C transactions will rely primarily on the industry's ability to ally the fears of the average consumer, sampling experts may not be appropriate. The oversight of young consumers who will likely drive the growth of e-commerce is actually a problematic sampling trend in the literature.

YouthStream Media Networks and Greenfield (2000) found that the vast majority of college students (81%) report having made an online purchase. Klewin's (2000) research suggests that computers are a way of life for Generation Xers (i.e. the 20-something group) and these consumers perceive online shopping as a convenience. Studies overlooking young consumers (i.e. the largest, most affluent, skeptical, and savvy customer base) may draw conclusions that do not reflect those who are more likely to use e-commerce (Dietz, 1999).

It should also be noted that past experience with the selected sites might have influenced individuals' responses to the surveys. Future studies should account for this possibility by measuring specific past experience with each of the sites under investigation. There could also be additional dimensions that may prove of importance in perceptions of trustworthiness, but which were not included in the present study. For example, benevolence should be examined in future studies. Finally, the measures of agreement between experts (in testing of Hypothesis 2) include one 'fair' agreement level. However, while the experts did not completely agree on the contents of their ratings, they came up with the exact same rating for the site's privacy. As a result, even though the inter-level agreement is not high, the results of the hypothesis test were not affected.

6. Conclusion

The growth of business to consumer electronic commerce seems to be non-stoppable. Yet, online consumer spending only accounts for about 1.7% of overall retail revenues. For the future growth of B2C electronic commerce, barriers such as security and privacy concerns must be torn down. The best way to get over barriers is to clearly understand how they work and why they exist. This research offers a beginning point to understanding the relationship and the balance between the three elements of trustworthiness, privacy and security in B2C e-commerce. Additional findings related to the quality of the Web sites are also gleaned from the initial research. Future research streams may begin to provide some additional insights into the nature of electronic trustworthiness, and ultimately specific ways to inspire it.

Acknowledgements

The authors would like to express their appreciation to Drs Jarvenpaa and Sambamurthy, as well as anonymous reviewers, for their insightful comments on earlier drafts of this manuscript.

References

Anonymous, Net users distrust corporate privacy policies-study, February, 19, 2002, available at http://www.newsbytes.com/cgi-bin/udt/im..ble?client.id = newsbytesandstory.id = 174596.

Ba, S., 2001. Establishing online trust through a community responsibility system. Decision Support Systems 31, 323–336.

Branscum, D., 2000. Guarding on-line privacy. Newsweek 135 (23), 77–78.

Carroll, A.B., 1979. A three-dimensional conceptual model of corporate social performance. Academy of Management Review 5, 497–505.

Cassell, J., Bickmore, T., 2000. External manifestations of trustworthiness in the interface. Communications of the ACM December, 50–56.

Cheskin Research and Studio Archetype/Sapient. eCommerce Trust Study, January 1999.

Cheung, C.M.K., Lee, M.K.O., 2001. Trust in internet shopping: instrument development and validation through classical and modern approaches. Journal of Global Information Management 9 (3), 23–46.

Conhaim, W.W., 1998. E-commerce. Link-Up 15 (1), 13–15.

Crosby, L.A., Evans, K.R., Cowles, D., 1990. Relationship quality in services selling: an interpersonal influence perspective. Journal of Marketing 54 (7), 68–81.

Dayal, S., Landesberg, H., Zeisser, M., 1999. How to build trust online. Marketing Management 8 (3), 64–71.

Dietz, J., 1999. When Gen X meets aging baby boomers. Marketing News 33 (10), 17–18.

Durvasula, S., Mehta, S.C., Andrews, J.C., Lysonski, S., 1997. Advertising beliefs and attitudes: are students and general consumers indeed different? Journal of Asian Business 13 (1), 71–84.

Edmondson, V.C., Carroll, A.B., 1999. Giving back: an examination of the philanthropic motivations, orientations and activities of large black-owned businesses. Journal of Business Ethics 19, 171–179.

Francis, D.F., 2000. Despite dotcom failures, E-tail's future is bright. Christian Science 20, 17.

Friedman, B., Kahn, P.H. Jr., Howe, D.C., 2000. Trust online. Communications of the ACM December, 34–40.

Garbarino, E., Johnson, M., 1999. The different roles of satisfaction, trust and commitment in customer relations. Journal of Marketing 63 (2), 70–87.

Gefen, D., 2000. E-commerce: the role of familiarity and trust. The International Journal of Management Science, Omega 28, 725–737.

Glass, A.D., 1998. A countdown to the age of secure electronic commerce. Credit World 86 (5), 29–31.

Green, H., Yang, C., Judge, P.C., 1998. A little privacy, please. Business Week 3569, 98–99.

Harris Interactive, Consumer privacy attitudes and behaviors survey wave II, The Privacy Leadership Initiative, July 2001a, http://www.understandingprivacy.org/content/library/harris2-execsum.pdf.

Harris Interactive, Why some companies are trusted and others are not: personal experience and knowledge of company more important than glitz, June 2001b, http://www.harrisinteractive.com/harris_poll/index.asp?PID = 237.

Hoffman, D., Novak, T.P., Peralta, M., 1999. Building consumer trust online. Communications of the ACM 42 (4), 80–85.

Houston, D.A., 2001. Trust in the networked economy: doing business on web time. Business Horizons March–April, 38–44.

Hosmer, L., 1995. Trust: the connecting link between organizational theory and philosophical ethics. Academy of Management Review 20, 379–403.

Ibrahim, N.A., Angelids, J.P., 1993. Corporate social responsibility: a comparative analysis of perceptions of top executives and business students. The Mid-Atlantic Journal of Business 29, 303–315.

Ibrahim, N.A., Angelids, J.P., Kuniamsky, H.R., 1997. Corporate social responsibility: a comparative analysis of perceptions of corporate directors in financial and manufacturing organizations. International Journal of Management 14, 590–597.

Jacobs, P., 1997. Privacy: what you need to know. InfoWorld 19 (44), 111–112.
Jarvenpaa, S.L., Tractinsky, N., Vitale, M., 2000. Consumer trust in an internet store. Information Technology and Management 1 (1), 45–71.
Kalakota, R., Whinston, A.B., 1996. Frontiers of Electronic Commerce, Addison-Wesley, Reading, MA.
Klewin, B., 2000. Gen Xers hold a few surprises. Credit Union Magazine 66 (2), 54–55.
Kuchinskas, S., 1999. In web sites we trust? Brandweek 40 (7), 46–48.
Landis, J.R., Koch, G.G., 1977. The measurement of observer agreement for categorical data. Biometrics 22, 79–94.
Lee, M.K.O., Turban, E., 2001. A trust model for internet shopping. International Journal of Electronic Commerce 6 (1), 75–91.
Lohse, G., Spiller, P., 1998. Electronic shopping. Communications of the ACM 41 (7), 81–87.
Lynch, P.D., Kent, R.J., Srinivasan, S.S., 2001. The global internet shopper: evidence from shopping tasks in twelve countries. Journal of Advertising Research May/June.
Mayer, R., Davis, J., Schooman, F., 1995. An integrative model of organizational trust. Academy of Management Review 20, 709–734.
Miyazaki, A.D., Fernandez, A., 2000. Internet privacy and security: an examination of online retailer disclosures. Journal of Public Policy and Marketing 19 (1), 54–61.
Miyazaki, A.D., Fernandez, A., 2001. Consumer perceptions of privacy and security risks for online shopping. The Journal of Consumer Affairs 35 (1), 27–44.
Moorman, C., Deshpande, R., Zaltman, G., 1993. Factors affecting trust in market relationships. Journal of Marketing 57 (1), 81–101.
Muysken, J., 1998. Web trust: assurance and e-commerce. Australian CPA 68 (7), 56–57.
Ovans, A., 1999. Is Your web site socially savvy? Harvard Business Review 77 (3), 20–21.
Papadopoulou, P., Andreou, A., Kanellis, P., Martakos, D., 2001. Trust and relationship building in electronic commerce. Internet Research: Electronic Networking Applications and Policy 11 (4), 322–332.
Pastore, M., 2001. Privacy remains a concern for online consumers. CyberAtlas June http://cyberatlas.internet.com/markets/advertising/print/0,5941-781741,00.html.
Paul, P., 2001. Mixed signals. American Demographics 23, 44–49.
Ratnasingham, P., Kumar, K., 2000. Trading Partner Trust in Electronic Commerce Participation, Proceedings of the International Conference on Information Systems, Brisbane, Australia,.
Reynolds, H.T., 1977. The Analysis of Cross Classifications, Free Press, New York.
Sacharow, A., 1998. Create your own internet. Adweek 39 (19), 44–46.
Singh, J., Sirdeshmukh, D., 2000. Agency and trust mechanisms in consumer satisfaction and loyalty judgments. Journal of the Academy of Marketing Sciences 28 (1), 150–167.
Smith, W., Wokutch, R., Harrington, K., Bryan, D., 2001. An examination of the influence of diversity and stakeholder role on corporate social orientation. Business and Society 40 (3), 266–298.
Urban, G.L., Sultan, F., Qualls, W.J., 2000. Placing trust at the center of your internet strategy. MIT Sloan Management Review (1), 39–48.
Wang, H., Lee, M.K.O., Wang, C., 1998. Consumer privacy concerns about internet marketing. Communications of the ACM 41 (3), 63–70.
Wingfield, N., 2001. As web sales grow, mail-order sellers are benefiting most. Wall Street Journal May, B.8.
Woodlock, P., 1999/2000. Will my client benefit from webtrust? The National Public Accountant 44 (10), 46–49.
YouthStream Media Networks and Greenfield. The Internet Is 'Big Man on Campus'—New Study from Greenfield Online Reveals the Web is Huge on Campus—, 2000, http://www8.techmall.com/techdocs/TS000807-2.html.