Decision Support Systems 48 (2010) 407–418

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

The effects of Web assurance seals on consumers' initial trust in an online vendor: A functional perspective

Xiaorui Hu [a,*], Guohua Wu [b], Yuhong Wu [c], Han Zhang [d]

[a] Saint Louis University, United States
[b] California State University, Fullerton, United States
[c] Houston, Texas, United States
[d] Georgia Institute of Technology, United States

ARTICLE INFO

Article history:
Received 26 February 2007
Received in revised form 28 July 2009
Accepted 17 October 2009
Available online 24 October 2009

Keywords:
E-commerce
Web assurance seal
Initial trust
Privacy
Security
Transaction integrity

ABSTRACT

This research examines the effects of third-party Web assurance seals on consumers' initial trust in online vendors from a functional perspective. The main effects and interaction effects of different seal functions (i.e., privacy assurance, security assurance, or transaction-integrity assurance) on consumers' initial trust are explored. We constructed a $2\times2\times2$ between-participants full factorial design to conduct this lab-controlled experiment. The results demonstrate that there is an interaction between the privacy and security assurance functions such that the effect of either function on enhancing consumers' initial online trust is weakened by the presence of the other. Privacy and transaction-integrity assurance functions interact in a similar way. Consequently, Web assurance seals with multiple functions are not necessarily more effective than single-function seals in enhancing consumers' initial online trust. As the combined-function seals are currently offered in the e-markets, this finding provides insight to both Web assurance seal providers and online vendors who adopt or intend to adopt a Web assurance seal.

1. Introduction

Electronic commerce (e-commerce) is growing rapidly despite the dismal economy in recent years. According to the U.S. Census Bureau, total e-commerce sales for 2008 reached $133.6 billion [56]. However, U.S. e-commerce sales in 2008 still accounted for a meager 3.3% of total retail sales [56]. To reach its full potential, e-commerce must overcome many challenges. One key challenge is how to build online trust to alleviate risks associated with online transactions.

Consumers remain cautious about disclosing personal information online. Consumers perceive shopping online to be riskier than offline because they cannot visit a physical vendor and feel and touch products prior to purchase [57]. Issues such as the security of information and disclosure of information during and after the transaction process also tend to amplify online consumers' perceived risks [8,14,18], which corroborate well with actual online fraud statistics. For example, the FBI's Internet Crime Complaint Center (IC3) received 206,884 consumer complaints about alleged online fraud or cyber crime during 2007, and referred 90,008 complaints of crime to federal, state, and local law enforcement agencies for further investigation [22]. Non-delivery of merchandise and/or payment, credit and debit card fraud and identity theft were all among the 2007 top ten IC3 complaint categories [22]. Risks associated with e-commerce lead to serious trust concerns in electronic markets (e-markets) [3,19,20], which hinder the growth of e-commerce to its potential.

Both practitioners and academic researchers in e-commerce have attempted diverse intervention strategies to promote online trust. One strategy adopts a third-party Web assurance seal to signal institution-based trustworthiness [35], particularly for small online retailers [58]. The academic literature, however, presents a pattern of inconsistent findings with regard to the effects of Web assurance seals on online consumer trust. For example, some previous studies find significant and positive impacts of Web assurance seals on consumer trust (e.g., [30,42,44,53]), while others do not find a significant impact (e.g., [21,24,27,35,48,58]). Thus, more research is warranted.

We make a unique contribution with our study by taking a functional perspective in examining the effects of Web assurance seals on consumer trust enhancement. We focus on three major assurance functions served by Web assurance seals: (1) transaction security assurance (e.g., VeriSign), (2) consumer privacy assurance (e.g., TRUSTe), and (3) transaction-integrity assurance (e.g., BBB*OnLine* Reliability) [25,27]. This functional approach allows us to conduct an in-depth analysis of the complexity of Web assurance seals and to assess the impact of each assurance function on consumer trust [10].

* Corresponding author.
E-mail addresses: hux2@slu.edu (X. Hu), mwu@fullerton.edu (G. Wu), yuhong_ut@yahoo.com (Y. Wu), han.zhang@mgt.gatech.edu (H. Zhang).

0167-9236/$ – see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.dss.2009.10.004

More importantly, such a functional approach enables us to reveal whether different assurance functions combined in one Web seal interact with each other, and whether the interactions among those functions strengthen or weaken the effect of each function on enhancing consumers' initial online trust.

Due to the nature of the experiment, it is unlikely that we will incorporate participants' experience and their firsthand knowledge about an online vendor, each of which are required to form general trust [34]. Therefore, we focus our study on consumers' initial online trust, which is referred to as consumers' initial trust in the rest of the paper. A consumer's initial trust "will not be based on any kind of experience or firsthand knowledge of" the online vendor, but it will be based on his or her own "disposition to trust or on institutional cues" [34]. Empirically, this study focuses on the period during which a consumer visits and explores an online vendor's Web site for the first time and falls within the domain of initial trust [33,35].

Accordingly, the primary purpose of this study is to examine the main effects and the interaction effects of the three Web assurance functions on consumers' initial trust. Specifically, we are interested in understanding (1) whether each of the three Web assurance functions enhances consumers' initial trust and (2) when two or more assurance functions are combined in a seal, whether there will be a synergistic interaction among them on enhancing consumers' initial trust, such that the effect of either function will be stronger than that in a single assurance function seal.

The remainder of the paper is organized as follows. Section 2 reviews the current literature on trust and Web assurance seals. Section 3 presents the hypothesis development. Section 4 discusses the research methodology. Section 5 presents the findings and Section 6 concludes the paper with discussion of the research implications for online vendors and Web assurance seal providers, the limitations of current research, and suggestions for future research.

2. Literature review

Trust is a focal construct in exchange relationships. The concept of trust includes trusting beliefs and trusting intention, and trusting beliefs lead to trusting intention [34]. Trust starts with a belief and an expectation that another party will behave in a credible or benevolent manner [1,13]. Thus, one party which trusts a second party is willing to rely on and depend on that party in spite of uncertainty [23,40].

Trust plays a key role in the relationship between two parties. For example, Ganesan [15] finds that trust is an important factor in determining the long-term orientation of a retailer and its vendors. Doney and Cannon [13] propose that trust is positively related to a buyer's anticipation of future interactions with the supplier. Indeed, trust impacts a party's commitment to a relationship [41].

Trust is widely recognized as a key factor in facilitating online transactions [4,16,17,23,54]. Indeed, a trade cannot even be initiated without sufficient trust. Lesser-known online vendors, in particular, face a more formidable challenge of inducing an adequate level of initial trust to convince online consumers to complete any transaction. Thus, a lesser-known online vendor should seek to provide opportunities for online consumers to assess its trustworthiness and to engender sufficient initial trust from them so that a trade can be established [33,35].

Several studies explore the factors that impact establishment of such initial trust. Concentrating on antecedents of initial trust, Koufaris and Hampton-Sosa [29] find that perceived company reputation and willingness to customize products and services can significantly affect consumers' initial trust. Moreover, perceived Web site usefulness, ease of use and security control are also significant antecedents of consumers' initial trust. McKnight et al. [35] find that disposition to trust, structural assurance (institution-based trust), and reputation advertising have significant effects on consumers' initial trust in the Web business. Bahmanziari et al. [6] explore the most important factors in the formation of consumers' initial trust for technology adoption decisions. They find that a money back guarantee, customer help/online assistance, and availability of training can significantly affect consumers' initial trust.

Other studies examine the antecedents and consequences of consumers' trust in an online vendor without a specific focus on initial trust. These studies also provide important insights into how trust is formed and why these factors are important. Jarvenpaa et al. [23] find that consumers can perceive differences in size and reputation among online vendors. Those differences affect their assessment of a vendor's trustworthiness, perceptions of risk, and their willingness to purchase from the vendor. Gefen [16] proposes that familiarity with and trust in an online retailer influence consumer intentions to both inquire about the retailer's merchandise and purchase from the retailer. Balasubramanian et al. [7] find that perceived trustworthiness of an online broker significantly affects investors' satisfaction. Gefen et al. [17] argue that consumers' trust in an online vendor and their assessment of the information technology play important roles in determining consumers' online purchasing intentions. While exploring how trust is transferred across hypertext links and from physical to virtual vendors, Stewart [54] suggests that consumers' willingness to buy from an online vendor is an outcome of both trust in that vendor and perceived Internet-related risk.

Recently, the use of Web assurance seals as an institutional cue to engender consumer trust has drawn attention in academic research (e.g., [10,30,35,38,39]). Table 1 summarizes the major findings from these empirical studies on Web assurance seals. These previous studies have made important contributions toward our understanding of whether Web assurance seals enhance consumers' online trust but their findings are inconsistent.

3. Hypothesis development

3.1. Conceptual background

An online vendor adopts one or more third-party Web assurance seals as a cue to signal its trustworthiness to its potential customers [58]. This "cue" perspective suggests that cue utilization theory [11,46] and cue consistency theory [2,31] might serve as a useful framework through which we can obtain a clear understanding of how online consumers perceive Web assurance seals as trust-enhancing cues. Previous research has used both the cue utilization theory and cue consistency theory to examine consumers' perceptions of product quality (e.g., [37,52]). Our study intends to investigate consumers' perceptions of trustworthiness of an online vendor, which are central to consumers' quality perceptions of the online vendor, which, in turn, affect their purchasing intention. Therefore, we use these theories as a foundation to develop research hypotheses in this paper.

3.1.1. Cue utilization theory and cue consistency theory

The cue utilization theory suggests that a product sends out a series of cues signaling its quality to consumers [11,46]. Cues can be categorized as extrinsic or intrinsic to the product [47]. Extrinsic cues are product-related attributes but can be altered, whereas intrinsic cues are inherent to the product itself (e.g., ingredients) and cannot be easily altered. Intrinsic cues generally dominate extrinsic cues [50,51]. However, if intrinsic cues are missing, not very useful, or not being processed, consumers are more likely to use extrinsic cues to assess product quality [37].

Likewise, when an online shopper visits an unknown online vendor for the first time, his or her evaluation of the online vendor's trustworthiness will be based upon both intrinsic and extrinsic cues present on the online vendor's Web site. An online vendor's intrinsic cues can come from the kinds of products and/or brands it carries. An

Table 1
Summary of major empirical studies on Web assurance seals.

Citation	Seals in research	Principal questions	Findings
Kovar et al. [30]	Real seal: WebTrust	What is the influence of assurance services on consumers' online transaction expectations and intent to purchase online?	Consumers who pay more attention to the seal and its disclosures at the retailer's Web site, or who have been exposed to WebTrust advertising, have higher online transaction expectations and a stronger willingness to buy than their counterparts.
Noteberg et al. [42]	Hypothetical seals (accountant's assurance, consumer union's assurance, and computer industry's assurance)	What is the impact of third-party-provided electronic commerce assurance on consumers' likelihood to purchase products and services online and their concerns about privacy and transaction integrity?	E-commerce assurance provided by third parties significantly increases consumers' purchasing likelihood and reduces consumers' concerns about privacy and transaction. However, among various third-party assurance providers (e.g., an independent accountant, bank, computer industry, or consumer union), no significant differences toward influencing consumers' trust is found.
Odom et al. [44]	Real seals: VeriSign, TRUSTe, Good Housekeeping, and CPA WebTrust	Is there a positive relationship between consumers' 1) recognition of and 2) familiarity with a Web assurance seal and online purchasing decision?	For all other seal brands except for CPA WebTrust seal, there exists a positive relationship between 1) recognition of and 2) familiarity with a Web assurance seal and consumers' online purchase decision.
Rifon et al. [53]	Real seals: TRUST*e* and BBB*Online* privacy seal	What is the ability of privacy seals to signal information practices when information practices are unavailable and not known?	Privacy seals enhance trust in the Web site and expectations that the site would inform the user of its information practices.
Pennington et al. [48]	Real seals: Bizrate and Better Business Blue Ribbon	What is the possible impact of Web assurance seals on system trust in B2C transactions?	The seals do not have significant impact on system trust in B2C transactions.
Kimery and McCord [27]	Real seals: VeriSign, TRUST*e*, and BBB reliability	Is there a positive relationship between an assurance seal and consumers' trust in the e-retailer?	There is no significant relationship between Web assurance seals and consumers' trust.
Wang et al. [58]	Real seals: TRUST*e*, BBB*OnLine*, and VeriSign	Is consumers' cue-based trust in an online retailer positively related to the presence of seals of approval on its Web site?	A third-party assurance seal cannot significantly increase consumers' cue-based trust.
McKnight et al. [35]	Real seals: TRUST*e* and ATLA (Association of Trial Lawyers of America)	Do the use of privacy icons and the use of industry seals increase consumers' initial trust in a Web-based business?	Neither a noticeable TRUST*e* privacy seal nor a noticeable professional association seal has any significant impact on consumers' initial trust in the Web business.
Kim et al. [26]	Real seals: VeriSign, TRUST*e*, BBB*OnLine* Privacy, Online Privacy Alliance, WebTrust, etc.	Does an intervention to educate consumers about Web site security features (i.e., privacy, security practices, information quality, and Web assurance seal services) affect consumers' perception of the Web site security features?	Educating consumers about the security and privacy dangers of the Web, as well as the role of Web assurance seals, increases their awareness and perceived importance of the seals. However, despite this increased awareness, no significant relationship is found between the assurance seals and the two indicators of trustworthiness, concerns about privacy and perceived information quality of an e-commerce site, even after the intervention.
Hui et al. [21]	Real seal (TRUST*e*) and privacy statement	Do consumers value privacy statements and privacy seals? If so, do these statements and seals affect consumer disclosure of personal information?	The existence of a privacy statement induces more subjects to disclose their personal information, but that of a privacy seal does not.

online consumer may develop a certain level of initial trust when he or she sees name brands being sold by an online vendor. However, the very nature of online shopping makes it unlikely for consumers to examine products with their senses (e.g., touch, smell) other than viewing the image of a product. Consequently, there are few intrinsic cues available to consumers, who in turn rely more on extrinsic cues to assess the trustworthiness of the online vendor. Extrinsic cues may encompass customer testimonials, ratings, and various assurances provided by independent third-party endorsements such as Web assurance seals. In our study, the various assurance functions carried by Web assurance seals work as extrinsic cues signaling the trustworthiness of an online vendor.

When multiple cues are present, the cue consistency theory provides some understanding about how consumers jointly apply these cues in their evaluation and decision making process. The cue consistency theory holds that when consumers encounter multiple sources of information that corroborate one another, consumers tend to jointly evaluate the information through an information integration model, such as linear averaging [2,31]. That is, when multiple consistent cues are presented to a consumer, each cue tends to receive more attention and weight in the consumer's evaluation. However, when cues are not consistent (i.e. one positive/one negative or one weak/one strong), the negative or weak cue tends to dominate consumers' evaluation. For example, Miyazaki, Grewal, and Goodstein [37] find that when high price — an extrinsic cue of product quality — is paired with another positive extrinsic cue (such as a strong warranty or a strong brand name), a synergistic interaction exists between them, in which the effect of either cue is strengthened by the presence of the other (given that intrinsic information is scarce). As an online vendor could address online shoppers' various concerns through multiple assurance functions, the cue consistency theory thus provides insights on how the multiple cues work together in consumers' trust development process.

3.2. Research hypotheses

Third-party endorsement from trusted sources is believed to signal the trustworthiness of an online vendor displaying such seals [30,42,44,53]. When online consumers see such Web assurance seals displayed on an unknown online vendor, they are likely to use these seals as extrinsic cues to infer the trustworthiness of the online vendor through the following two processes — trust transference and intentionality [13,58]. Trust transference posits that a trusting party develops trusting beliefs by depending on the "proof sources" of the trustee [13]. Similarly, an online consumer is likely to use the trusted reputation of seal issuers (e.g., TRUST*e*, VeriSign, and BBB*OnLine*) to perceive the credibility of the online vendor. Intentionality holds that a trusting party evaluates a trustee's motivations to make sure that the trustee is benevolent [13]. When an online consumer sees the display of Web assurance seals, he or she will infer that since these seal providers are well-known entities, online vendors choosing to be under the

scrutiny of these entities and willingly abide by their rules are unlikely to exploit consumers for a single transaction gain. In addition, a consumer can always click on the seal to verify whether the Web site owner is in fact in compliance with the standards and practices issued by the seal providers.

Previous studies suggest three major issues in online transactions: (1) the issue of privacy [25,27,36,42], (2) the issue of security [25,27,36], and (3) the issue of transaction integrity. The third issue reflects consumers' concerns over an online vendor's motivation and ability to handle order fulfillment [25,27,42]. In practice, Web assurance seals attempt to address one or more of these three concerns. A privacy assurance function is used to alleviate online consumers' perceived risk of leaking personal identification information. For example, TRUST*e* provides a privacy assurance seal assuring that any Web site displaying its symbol conforms to its privacy standards. A security assurance function reassures online consumers that the online vendor uses a special protocol (e.g., HTTPS) to secure online transactions and a secured database to protect their personal information. For instance, VeriSign assures users that any Web site displaying its symbol complies with its encryption and authentication standards. A transaction-integrity assurance function guarantees fair business practices and business transactions before, during, and after the online transaction. For example, BBB*OnLine* assures customers that any Web site displaying its symbol abides by the rules set up by Better Business Bureau in the online context.

Therefore, an online vendor who displays a Web assurance seal addressing one of the following assurances, privacy, security, or transaction integrity, can be viewed as providing an extrinsic cue to signal the trustworthiness of the online vendor to its online consumers. Based on the above discussions, we can expect an increase in consumers' initial trust toward an online vendor adopting such a seal.

Thus, we propose:

H1. The display of a seal containing a privacy assurance function significantly increases consumers' initial trust in an online vendor.

H2. The display of a seal containing a security assurance function significantly increases consumers' initial trust in an online vendor.

H3. The display of a seal containing a transaction-integrity assurance function significantly increases consumers' initial trust in an online vendor.

Online vendors can use Web seals with various assurance function(s) to signal trustworthiness to potential customers. Each assurance function – privacy, security, or transaction integrity – can be considered as an extrinsic cue reducing one of the major concerns for online transactions. A third-party endorsed Web assurance seal can carry more than one of these assurance functions within a single seal. For instance, the BBB Accredited Business Seal assures that an online company meets and abides by the multi-dimensional standards of the BBB Code of Business Practices including privacy, security and business integrity [5]. The Trust Guard Certified Seal is also a stand-alone, multi-purpose seal, which assures privacy, security, and part of business integrity (e.g., requiring business address, managing member address, phone number, email address, etc.) [55]. Based on the cue consistency theory which is discussed earlier, these various assurance functions can be considered consistent cues that provide corroborating information to mitigate online consumers' anxiety and/or perceived risk. Consequently, we predict that a synergistic interaction exists when two assurance functions are combined in a seal, such that the relationship between each assurance function and consumers' initial trust is more pronounced. That is, when a seal contains two assurance functions, the effect of either assurance function on consumers' initial trust is strengthened or elevated by the presence of the other assurance function.

Further, when three assurance functions are combined in one seal, we believe online consumers tend to perceive the three assurance functions as consistent cues reinforcing each other. Thus, we predict an interaction effect among these three assurance functions, such that the projected interaction effects between any two of the three assurance functions could be strengthened by the presence of the third assurance function. Based on the preceding arguments, we propose the following hypotheses:

H4. When a seal contains a privacy and a security assurance functions, there will be an interaction between these two functions in enhancing consumers' initial trust, such that the effect of either function is stronger with the presence of the other assurance function than without.

H5. When a seal contains a privacy and a transaction-integrity assurance functions, there will be an interaction between these two functions in enhancing consumers' initial trust, such that the effect of either function is stronger with the presence of the other assurance function than without.

H6. When a seal contains a security and a transaction-integrity assurance functions, there will be an interaction between these two functions in enhancing consumers' initial trust, such that the effect of either function is stronger with the presence of the other assurance function than without.

H7. When a seal contains a privacy, a security, and a transaction-integrity assurance functions, there will be an interaction among these three functions in enhancing consumers' initial trust, such that the interaction of any two assurance functions is stronger with the presence of the third assurance function than without.

4. Methodology

4.1. Experimental design

We used a 2 (presence vs. absence of a privacy assurance function) × 2 (presence vs. absence of a security assurance function) × 2 (presence vs. absence of a transaction-integrity assurance function) between-participants full factorial design to test the above hypotheses. We designed a Web site with a professional "look and feel" to simulate a real online shopping experience. The Web site contained the following six tabs: "Home," "Company," "Products," "Customer Services," "Return Policies," and "Contact Information." We carefully chose products featured through the online vendor that bore direct relevance to the experimental participants (i.e., college students). Products included textbooks, computers, apparel (sports shoes), accessories, and perfume. In each category, we listed three brand-name products and the price we offered was 20% lower than the current market price. Using the 20% discount as an incentive is a practice widely used in marketing and advertising (e.g., [9]).

Eight versions of the Web site were used in the experiment. One version of the Web site had no seal displayed and was called the control condition. Participants who viewed this version were referred to as the control group. The other seven versions served as treatment conditions and all had a Web assurance seal named "CyberTrust," displayed prominently on the Web site. We include a screenshot of the home page of one version of the Web site that featured a CyberTrust seal in Appendix A.

We informed the participants in the treatment groups that the CyberTrust seal was provided by Consumer Reports. One page of description about Consumer Reports was distributed to the participants and adequate time was given to them to read through the information. Administrators affirmed to the participants that Consumer Reports was a trustworthy third party. In doing so, we aimed to control the different degrees of trust transfers associated with Consumer Reports among subjects.

The seven treatment conditions differed in the type and number of assurance functions contained in the CyberTrust seal. The home pages for all seven treatment conditions had the exact same appearance, and the CyberTrust seal was posted on the same position on each version of the Web site. Only when participants clicked on the seal would a separate page pop up, revealing the description of the different assurance function(s) (See Appendix B). We studied the descriptions provided by WebTrust, VeriSign, and BBB*OnLine* Seals, and developed the descriptions of our assurance functions. Specifically, three treatment conditions had the seal containing only one assurance function (i.e., privacy assurance, security assurance, or transaction-integrity assurance, respectively); three others had a seal that included a combination of two assurance functions (i.e., a privacy assurance plus a security assurance, a privacy assurance plus a transaction-integrity assurance, or a security assurance plus a transaction-integrity assurance); the last version had a seal that included all three of the assurance functions.

We conducted a pilot test to improve the Web site design, navigation, and the survey questionnaire. Thirty undergraduate students from a university in the United States were recruited on a voluntary basis for the pilot test.

4.2. Participants

We recruited college students to participate in this experiment. One hundred and eighty-five undergraduate students from two different universities in the United States participated in the main study. Participants were randomly assigned to each of the eight experimental conditions. Of the participants, 44% were female, and the majority (91.3%) was between the ages of 18 and 35. The participants' Web surfing skills were relatively high (mean = 5.84, S.D. = 1.03, on a 7-point Likert scale with 1 = lowest and 7 = highest). 77% of them had shopped online in the past 6 months.

4.3. Procedures

Before the experiment began, experiment administrators opened different versions of the Web site in Internet browsers. Then, we asked the participants to enter the computer lab and take a seat randomly. The Web site was also shown on a screen controlled by an LCD projector. Since the control group's Web site had no seal on it, we ran the experiment of the control group either in a separate computer lab or at a different time from the other treatment groups.

For the control group, the LCD projector displayed the control group's homepage, which had no seal on it. For the seven treatment groups, the LCD projector displayed the Web site with the CyberTrust seal displayed just above the horizontal navigation bar. The seven treatment groups were exposed to an identical Web site, except that when participants clicked on the CyberTrust seal, a different assurance function(s) was displayed, as described earlier. For example, one of the seven treatment groups would see a privacy assurance function after they clicked the CyberTrust seal, while another group might view a combination of privacy and security assurance functions. In addition, the participants did not know that different screens displayed different seal descriptions — only the administrator knew which participant had what version.

After the participants sat at the computers, they were told specifically NOT to click the navigation buttons on their own. Instead, administrators directed participants to click the navigation buttons one at a time ("Home," "Company," "Products," "Customer Service," "Return Policy," "Contact Information"), as well as the seal button (if present) on the top of the Web site. They were asked to carefully read all of the information after clicking each button, and an adequate amount of time was allocated to each button. The directed browsing of the Web site took about 15 minutes. This process ensured that the participants had equal chances to learn the information under each menu button and the seal button. By embedding the clicking of the seal button within the sequence of the clicking of other menu buttons, we minimized demand effects. Meanwhile, we realized that a lack of attention to a seal description may yield invalid research results [28]. Therefore, we asked participants to carefully read through the description of the contents displayed in each button as well as the assurance function(s) in the seal.

After the directed browsing, participants were asked to freely explore any part of the Web site for an additional 5 min. Participants were then instructed to fill out a questionnaire minutes their perceived initial trust. Then, a separate questionnaire was distributed to collect information about the participants' demographic information, their Web usage and online shopping experience, etc. Finally, the participants were debriefed and thanked for their participation.

Each experimental session took approximately 50 minutes. One hundred and eight-five completed survey questionnaires were collected during 12 sessions; each session ranged from 5 to 30 participants.

5. Analysis and results

5.1. Measures

We asked the participants to report their perceived trust in doing business with the hypothetical online vendor. We measured perceived trust in the online vendor by five items adapted from Doney and Cannon [13] and Pennington et al. [48]. The construct items of the perceived trust are recorded in Appendix C. All items were on a seven-point Likert-type scale, and we averaged the five items to formulate the perceived trust variable. The Cronbach alpha for the scale is 0.91 for perceived trust, higher than the 0.70 cut off point that Nunnally [43] suggests.

For manipulation checks, we followed O'Keefe [45] and Perdue and Summers [49]. As the presence of an assurance seal was self-evidently different from the absence of an assurance seal, no manipulation check was deemed necessary [45,49]. Meanwhile, as the subjects' attention to the seal description was crucial to our experiment, we checked and made sure that all of our participants followed the instructions in terms of clicking each button and viewing the pages. We gave participants enough time to read and comprehend the presented information during the directed navigation.

5.2. Results

Six of the 185 responses omitted values on the variable of consumers' initial trust. Therefore, we used the remaining 179 responses to perform the data analysis. We conducted this experiment at two different campuses, and we were aware that our results might be confounded by a possible campus effect. Our full factorial analysis of variance shows no significant main effect of campus ($F_{1,\ 163} = 2.04$, $p = 0.12$), and the campus factor shows no interaction with any of the three main factors (i.e., privacy, security, and transaction-integrity). Thus, we eliminated the possible

Table 2
The ANOVA with consumers' initial trust as a dependent variable.

Source	Type III sum of squares	df	Mean square	*F*	*p*-value
Privacy assurance	0.932	1	0.932	0.611	0.436
Security assurance	4.050	1	4.050	2.652	0.105
Transaction-integrity assurance	8.483	1	8.483	5.555	0.020
Privacy × security	8.980	1	8.980	5.881	0.016
Privacy × integrity	6.571	1	6.571	4.303	0.040
Security × integrity	1.149	1	1.149	0.753	0.387
Privacy × security × integrity	0.343	1	0.343	0.225	0.636

confounding factor of a campus effect in our data analysis and combined the data collected from two campuses.

To analyze the main and interaction effects in a three-factor design, we followed the guidelines provided by MaxWell and Delaney [32]. We used a GLM (General Linear Model) to conduct a three-way ANOVA (analysis of variance) on the dataset with consumers' initial trust as a dependent variable and the three assurance functions – privacy assurance, security assurance, and transaction-integrity assurance – as the fixed factors. Table 2 shows the ANOVA results.

Hypothesis 7 states that when a seal contains privacy, security, and transaction-integrity assurance functions, there will be a synergistic interaction among these three functions in terms of enhancing consumers' initial trust. However, the statistic result in Table 2 shows that the three-way interaction is not statistically significant ($F_{1,\ 171}=0.225$, $p>0.05$). Thus, Hypothesis 7 is not supported.

Hypotheses 4 through 6 anticipate significant synergistic interactions between any two of the three assurance functions (i.e., privacy and security, privacy and transaction-integrity, and security and transaction-integrity). The ANOVA results suggest one non-significant two-way interaction (security and transaction-integrity), and two significant two-way interactions (privacy and security, privacy and transaction-integrity). We will examine each in detail in the following paragraphs.

No significant interaction exists between the security and the transaction-integrity assurance functions ($F_{1,\ 171}=0.75$, $p>0.05$). Fig. 1 demonstrates visually that the effect of the transaction-integrity (security) assurance function on enhancing consumers' initial trust does not change significantly whether security (transaction-integrity) assurance function is present or absent. Consequently, Hypothesis 6 is not supported.

The other two two-way interactions are significant ($F_{1,\ 171}=5.88$, $p<0.05$ for privacy and security interaction; $F_{1,\ 171}=4.30$, $p<0.05$ for privacy and transaction-integrity interaction), but the direction of the interactions is contrary to what has been hypothesized. That is, we find two attenuating interactions rather than synergistic interactions. Specifically, combining a privacy function with either a security or a transaction-integrity assurance function reveals an interaction effect on enhancing consumers' initial trust, such that the effect of either function is weakened. Therefore, Hypotheses 4 and 5 are not supported. Figs. 2 and 3 visually illustrate how the effects of security and transaction-integrity assurance functions vary depending on whether the privacy assurance function is present or absent.

Since all three assurance functions are involved in significant two-way interactions, none of the three main effects can be unambiguously interpreted. Further analyses are needed to shed light on these hypotheses.

We conducted several one-way ANOVA tests to explore how the effects of security and transaction-integrity assurance functions on consumers' initial trust vary at two levels of privacy assurance function (absence vs. presence). We find that when the privacy assurance function is present, the effect of the security assurance function on consumers' initial trust is non-significant ($F_{1,\ 90}=0.37$, $p>0.05$; mean of 4.98 versus 5.13), and the effect of the transaction-integrity assurance function is also non-significant ($F_{1,\ 90}=0.07$, $p>0.05$; mean of 5.09 versus 5.03). Conversely, when the privacy assurance function is absent, the effect of the security assurance function becomes significant ($F_{1,\ 85}=8.09$, $p<0.01$; mean of 5.29 versus 4.49), and the effect of the transaction-integrity assurance function also becomes significant ($F_{1,\ 85}=9.46$, $p<0.01$; mean of 5.33 versus 4.47). Thus, we confirm that the privacy assurance function has a moderating effect on both the security and the transaction-integrity assurance functions. Consequently, we cannot unconditionally support either Hypothesis 2 or Hypothesis 3, and both hypotheses are only partially supported. A seal with a security or transaction-integrity assurance function significantly increases consumers' initial trust when a privacy assurance function is absent.

As the privacy assurance function interacts with both the security and the transaction-integrity assurance functions, further analyses are needed before we can draw any conclusion with regard to Hypothesis 1. First, we conducted a one-way ANOVA at two different levels of the security assurance (presence vs. absence). We find that when the security assurance function is present, the effect of the privacy assurance function on consumers' initial trust is not significant ($F_{1,\ 87}=1.54$, $p>0.05$; mean of 4.98 versus 5.29); conversely, when the security assurance function is absent, the effect of the privacy assurance function on consumers' initial trust is significant ($F_{1,\ 88}=5.33$, $p<0.05$; mean of 5.13 versus 4.49). However, because of the two-way interaction

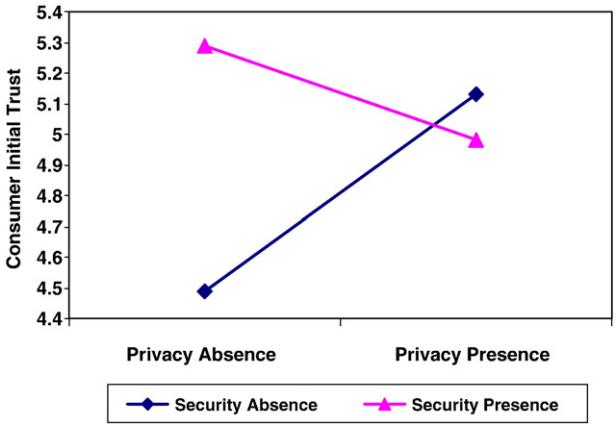


Fig. 2. Interaction between privacy and security assurance functions.

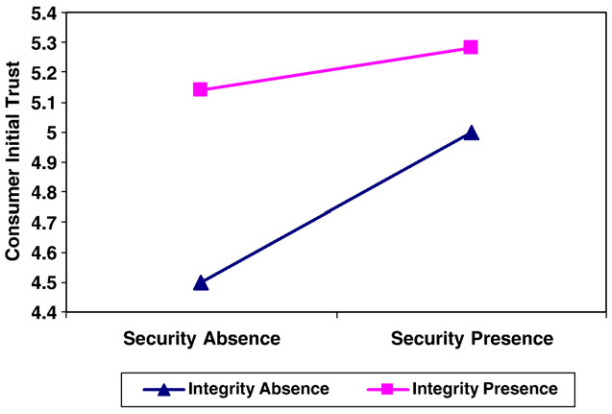


Fig. 1. No interaction between security and integrity assurance functions.

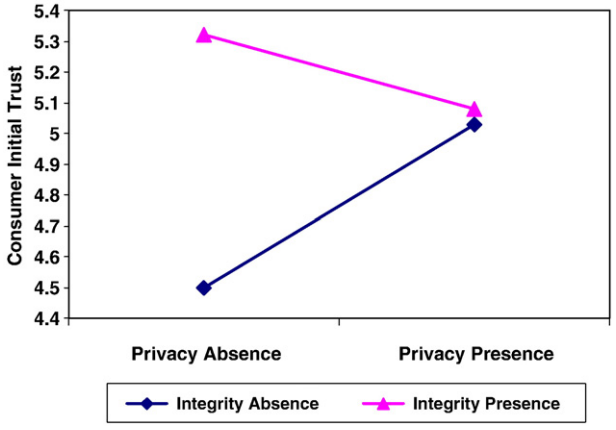


Fig. 3. Interaction between privacy and integrity assurance functions.

between the privacy and the transaction-integrity assurance functions, we need to conduct further analyses to isolate the role of the privacy assurance function from the potential effect of the transaction-integrity assurance function. Two *t*-tests reveal that the privacy assurance function has a significant effect ($t=2.64$, df = 43, $p<0.01$; mean of 5.07 vs. 4.00) only with the absence of both security and transaction-integrity assurance functions, whereas the privacy assurance function has a non-significant effect ($t=0.332$, df = 43, $p>0.05$; mean of 5.19 vs. 5.07) with the presence of the transaction-integrity function and the absence of the security assurance function.

Similarly, we conducted another one-way ANOVA for the privacy assurance function at two levels of the transaction-integrity assurance. We find that with the presence of the transaction-integrity assurance function, the effect of the privacy assurance on consumers' initial trust is not significant ($F_{1,\ 86}=0.96$, $p>0.05$; mean of 5.09 versus 5.33); and with the absence of the transaction-integrity assurance function, the effect of the privacy assurance on consumers' initial trust is marginally significant ($F_{1,\ 89}=3.97$, $p=0.05$; mean of 5.03 versus 4.47). We further conducted two *t*-tests to isolate the role of the privacy assurance function from the potential effect of the transaction-integrity assurance function because of the interaction between these two functions. We find that the privacy assurance function has a significant effect ($t=2.64$, df = 43, $p<0.01$; mean of 5.07 vs. 4.00) only with the absence of both the security and the transaction-integrity assurance functions, whereas the privacy assurance function has a non-significant effect ($t=-0.02$, df = 44, $p>0.05$; mean of 4.99 vs. 5.00) with the presence of the security assurance function and the absence of the transaction-integrity function.

Therefore, it appears that the effect of privacy assurance is complicated in its interactions with the other two assurance functions. Based on the preceding analyses, Hypothesis 1 can be partially supported under the condition of absence of the other two assurance functions.

Tables 3 and 4 summarize the cell means that provide a clear view of the complexity of the data.

The preceding results appear to refute the intuitive notion that a third-party Web assurance seal with more functions performs better than one with fewer functions. Thus we conducted a post hoc analysis to reveal further the relations between the number of assurance functions in a seal and their impact on consumers' initial trust.

A preliminary descriptive analysis shows an interesting relationship between the number of Web assurance functions in a seal and consumers' initial trust — it follows an inverted U-shaped curve (Fig. 4).

Fig. 4 shows the plot of means of consumers' initial trust corresponding to the number of assurance functions in one seal. For example, the mean of 5.04 is the average of the three means from which there is only one assurance function in the displayed seal, and the mean of 5.25 is the average of the three means from which there are two assurance functions in the displayed seal.

We also conducted a post hoc analysis using Tukey test, and the results suggest that there is a significant difference between a Web site displaying a seal (i.e. the seven treatment groups) and the one that does not (i.e. the control group) (see Table 5). This post hoc analysis empirically proves that a third-party Web assurance seal does help online vendors to boost consumers' initial trust, which supports the belief that displaying a third-party Web assurance seal is an effective strategy.

Table 3
Cell means and S.D. for the dataset with the privacy assurance absence.

Privacy absence			
	Integrity absence	Integrity presence	Marginal means
Security absence	4.00 (1.49)	5.07 (1.13)	4.49 (1.43)
Security presence	5.00 (1.23)	5.57 (1.12)	5.29 (1.20)
Marginal means	4.47 (1.45)	5.33 (1.14)	4.89

Note: the values are on a 7-point Likert scale and a higher value indicates a higher level of consumers' initial trust.

Table 4
Cell means and S.D. for the dataset with the privacy assurance presence.

Privacy presence			
	Integrity absence	Integrity presence	Marginal means
Security absence	5.07 (1.17)	5.19 (1.30)	5.13 (1.22)
Security presence	4.99 (1.28)	4.97 (1.03)	4.98 (1.16)
Marginal means	5.03 (1.22)	5.09 (1.17)	5.05

Note: the values are on a 7-point Likert scale and a higher value indicates a higher level of consumers' initial trust.

5.3. Discussion

Our research hypothesizes that the three different assurance functions (i.e., privacy, security, and transaction-integrity) serve as consistent cues signaling the trustworthiness of an online vendor to online consumers. We hypothesize that these consistent cues will not only have main effects but also have synergistic interaction effects in terms of boosting consumers' initial trust. Our results, however, portray an unexpectedly surprising and complex scenario.

We do not find any significant synergistic interactions in any of the combinations of assurance functions. Instead, we find two significant two-way interactions whose directions contradict our expectations: (1) attenuating interaction between the privacy and the security assurance functions (see Fig. 2) and (2) attenuating interaction between the privacy and the transaction-integrity assurance functions (see Fig. 3). These interactions suggest that the privacy assurance moderates the effects on consumers' initial trust of the other two assurance functions. Combining a privacy assurance function with either a security or a transaction-integrity assurance function weakens the effects of the other assurance functions on enhancing consumers' initial trust. Meanwhile, the effect of the privacy assurance function itself is weakened when it is combined with either one of the other two functions. Essentially, the privacy assurance function does not mix well with either the security or the transaction-integrity assurance function.

In fact, our detailed analyses indicate that the privacy assurance function has a significant positive impact on enhancing consumers' initial trust under only one condition — the absence of the other two assurance functions. In contrast, both the security and the transaction-integrity assurance functions have a significant positive impact on consumers' initial trust as long as the privacy assurance function is absent.

Now we want to explain the unexpected finding of the attenuating interaction between the privacy assurance function and the other two assurance functions when combined in a single seal. By revisiting the literature on the cue consistency theory, it could be that our assumption about the consistency among the three assurance functions as trust-

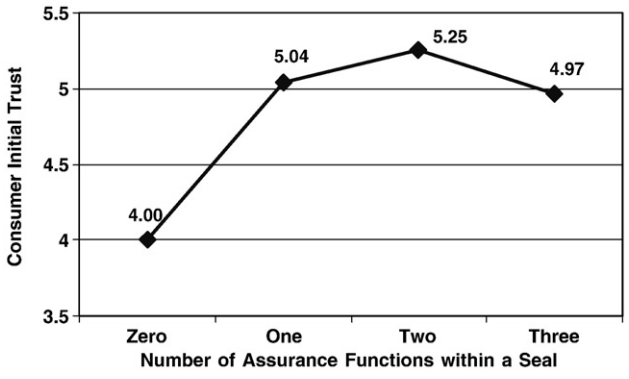


Fig. 4. The inverted U-curve of the number of assurance functions and consumers' initial trust.

Table 5
Tukey HSD test results for group comparison.

(I) Version Control group	(J) Version Treatment groups	Mean difference (I−J)	Std. error	Sig.
No seal	Privacy assurance	−1.07	0.38	0.03
	Security assurance	−1.00	0.38	0.05
	Transaction-integrity assurance	−1.07	0.39	0.03
	Privacy and security	−0.99	0.36	0.05
	Privacy and transaction-integrity	−1.19	0.36	0.01
	Security and transaction-integrity	−1.57	0.37	0.00
	Privacy, security, and transaction-integrity	−0.97	0.38	0.08

Dependent variable: consumers' initial trust.

signaling cues may not hold true. Indeed, we find a similar situation in which the hypothesized synergistic effects turn out to be weakening or attenuating effects (e.g., Dodds, Monroe, and Grewal's [12] study on the effects of price, brand, and store information on buyers' product evaluations). Then Miyazaki, Grewal, and Goodstein [37] offer a robust explanation by showing that when two inputs are not consistent, the overall assessment is not enhanced by the higher or stronger cue, and it is similar to that when both cues are weak. Perhaps the privacy assurance function is relatively weaker than either the security or the transaction-integrity assurance functions. Consequently, the relatively weak privacy assurance function becomes more salient and dominates consumers' overall trust perceptions of the online vendor when combined with the other relatively stronger cues.

One of our goals of this research is to reconcile the inconsistent findings regarding the effects of third-party Web assurance seals on consumers' initial trust. The attenuating interaction effects among the three assurance functions may help explain other non-significant effects in the third-party Web assurance seal research stream. For example, in the Wang et al. [58] study, no significant effect of seals of approval on cue-based trust was found. Although we cannot conclude that their three seals of approval are inconsistent cues, it may be that the privacy assurance function is not consistent with the other two Web assurance functions in terms of mitigating online consumers' concerns over online transactions.

6. Conclusion

In this study, we conducted a lab-controlled experiment to explore the main and the interaction effects of the three popular Web assurance seal functions (i.e., privacy assurance, security assurance, and transaction-integrity assurance) on enhancing consumers' initial trust. We find attenuating interaction effects rather than synergistic effects between the privacy and the security assurance functions and between the privacy and the transaction-integrity assurance functions. Such unexpected findings suggest that our intuitive notion about cue consistency among the three Web assurance functions might be questionable. In addition, we find that the effects of the security or the transaction-integrity assurance function on consumers' initial trust are moderated by the privacy assurance function. Without privacy assurance function, either the security or the transaction-integrity assurance function significantly increases consumers' initial trust. However, with the privacy assurance function, security or transaction-integrity assurance functions do not significantly increase consumers' initial trust. Meanwhile, privacy assurance has a significant positive impact on increasing consumers' initial trust only when both the security and the transaction-integrity assurance functions are absent. Overall, an online vendor can generate higher level of consumers' initial trust by displaying a Web assurance seal.

This study has theoretical and practical implications. First, theoretically, our functional perspective is unique in that it allows us to gain an in-depth understanding of how a trusted third-party issuing Web assurance seal transfers its trust to an unknown online vendor. Second, our functional perspective makes it possible to examine the effect of a single assurance function as well as the joint effects of two or three assurance functions, which provides valuable insights to seal providers and seal adopters. In particular, our counter-intuitive finding suggests that Web assurance seal adopters should be more cautious when combining privacy assurance with other assurance functions because it weakens the effects of the other assurance functions. This insight could help shed light on some inconsistent findings reported in the literature. In particular, for studies with non-significant results with regard to seal effects on consumers' initial trust, it is possible that the experimental stimuli (i.e., seals) may contain multiple functions that offset each other. Third, we believe that our research design allows for a more rigorous testing of the propositions. Our lab-controlled environment enhances internal validity, which is desirable given that the findings in previous literature are inconsistent. We eliminate several significant confounding variables, such as the familiarity and past experience with a seal, by using a hypothetical seal, CyberTrust, which participants presumed to be affiliated with Consumer Reports, a well-known public trust authority.

Our research findings present practical implications and guidelines for online vendors on their Web assurance seal adoption decisions. Our finding shows that there is a trust transfer, or an endorsement-like effect, of a third-party Web assurance seal for an online vendor displaying such a seal, which provides empirical justification for the very existence of the third-party Web assurance market. Therefore online vendors – small and lesser-known ones in particular, could consider adopting a Web assurance seal from a trusted third-party to help enhance their consumers' initial trust, which may result in more online transactions.

Meanwhile, choosing an appropriate seal could be a challenging task for an online vendor due to the diversity of Web assurance seals in the marketplace and the various cost structures associated with them. Though the more well-known Web assurance seals, such as TRUST*e*, VeriSign, and BBB*OnLine*, enjoy a first-mover advantage, an increasing number of new seals (e.g., SquareTrade, Thawte, GeoTrust, ESRB Privacy Certified, Trust Guard) have emerged in the Web assurance market. Some seal providers offer only one type of single-function seal (e.g., TRUST*e*'s privacy seal); some offer several different types of single-function seals (e.g., Trust Guard offers several types of seals, including privacy, security, and business verification seals); and some others offer a single assurance seal with multiple functions (e.g., BBB*Online*'s Trustmark, Trust Guard's Certified By seals). The cost structure of the seal providers may also vary. Some seal providers charge a fixed annual fee (e.g., GeoTrust[1] and Trust Guard[2]), while others charge a fee based on a company's annual revenue (e.g., TRUST*e*[3] and BBB*OnLine*[4]). In addition, bundle prices of multiple seals and seals with customized options are also available (e.g., Trust Guard).

Our research provides useful insights for seal adopters in choosing an appropriate seal. As different seal functions could weaken the effect of each other on enhancing consumers' initial trust, a multiple-function seal may not necessarily work more effectively than a single-function seal. In addition, the extra money paid (if any) for more assurance functions could be wasted and even counter-productive. Therefore, online vendors displaying Web assurance seals or planning to display such seals may not gain the expected additional benefits from purchasing multiple-function Web assurance seals. Rather, having one single-function seal may sufficiently generate an adequate level of initial trust among their customers. Meanwhile, our study also

[1] Please refer to http://www.geotrust.com/web_security/index.htm, last accessed on February 25, 2009.
[2] Please refer to http://www.trust-guard.com/trust-guard-seals-s/1.htm, last accessed on February 25, 2009.
[3] Please refer to http://www.truste.org/businesses/invoice_generator_coppa.php, last accessed on February 25, 2009.
[4] Please refer to http://us.bbb.org/WWWRoot/SitePage.aspx?site=113&id=d30d0ad2-4f6f-4a6b-bec6-594a441b25fe, last accessed on February 25, 2009.

suggests that seal providers, when designing Web assurance seals, should avoid combining assurance functions in a single seal to eliminate the possible attenuating interaction effects.

Like other studies in this research stream, this study has certain limitations. First, caution should be exercised when interpreting our findings because we used college student participants. We encourage a replication of this study using real online consumers in future research. Second, our study focused on the three major assurance functions — privacy, security, and transaction-integrity; however, other functions may deserve research attention as well. Odom et al. [44] find that the leading providers of online assurance seals address only a few of the online consumers' fears and concerns. A large gap exists between online consumers' actual needs for assurance and the perceived assurance offered by the seals. Some of these other functions might play a major role in promoting consumers' initial trust, which could be a future research direction. Third, our research also has the limitations associated with any laboratory experiment. For example, its external validity is not as high as a field experiment in which participants have a more realistic experience assessing their level of online trust. Future research could be conducted in a field study while participants actually purchase online from small online vendors with seals on vendors' Web sites. Finally, we must acknowledge that we did not randomize the order of Web assurance functions in a particular seal due to the small sample size. Future research could randomize the order with a larger sample size, and verify the results in this paper. Meanwhile, different assurance functions could be built in separate Web seals, and be presented side by side on a vendor's Web site as seen in current business practice. Studies could be conducted under this setting to reveal whether the attenuating effect among those functions still exists.

Acknowledgement

The authors would like to thank the three anonymous reviewers for their constructive comments. This research was partially supported by the CSU Summer Mini grant from San Jose State University for Guohua Wu.

Appendix A. Screenshot of the simulated Web site with CyberTrust seal

Appendix B. Three pop-up windows that contain seal function descriptions

CyberTrust Privacy Seal

The CyberTrust is a trusted authority affiliated with *Consumer Reports.*

You have arrived here from a CyberTrust certified site. The applicable CyberTrust Seal of Assurance symbolizes that this site has been examined by a CyberTrust professional. In order for an entity to be able to display the CyberTrust Seal of Assurance, it must meet one or more of the CyberTrust principles. The CyberTrust Seal of Assurance ensures that any Web site displaying it has met one or more standards established by CyberTrust.

The CyberTrust Seal of Assurance combines high standards for e-commerce activities with the requirement for a CyberTrust verification/audit. Together they build trust and confidence among consumers and businesses conducting business over the Internet. The entity has earned the right to display the Seal of Assurance with respect to the CyberTrust principle of:

Privacy:

Our standards demand that the entity disclose and comply with its on-line privacy practices. As a result, personally identifiable information obtained as a result of electronic commerce is protected and handled as promised. The entity never rents, sells or gives your personal information, including name, address, telephone number, e-mail address and, when necessary, credit card information and customer number, to any other organization for marketing purposes.

CyberTrust Security Seal

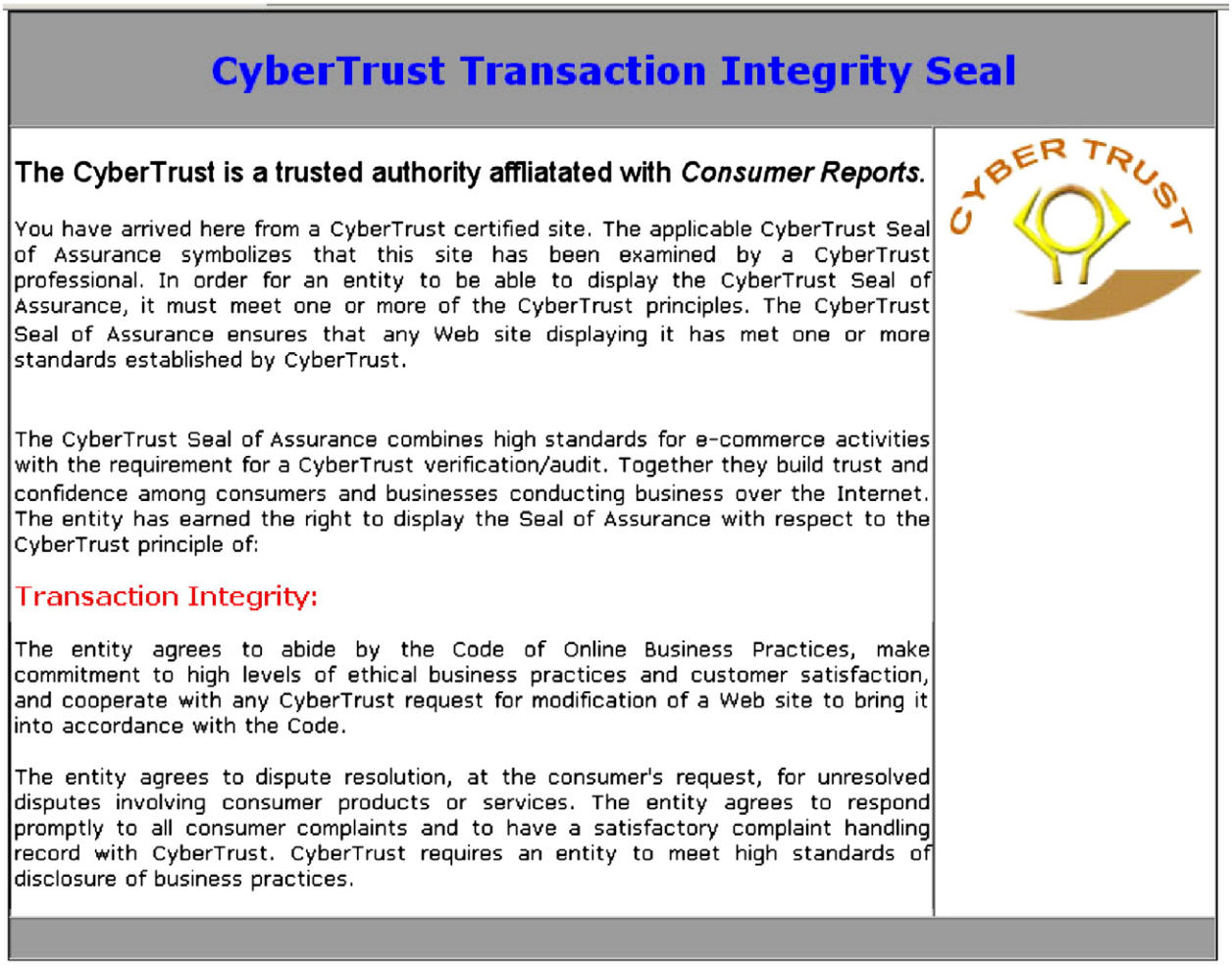
The CyberTrust is a trusted authority affiliated with *Consumer Reports.*

You have arrived here from a CyberTrust certified site. The applicable CyberTrust Seal of Assurance symbolizes that this site has been examined by a CyberTrust professional. In order for an entity to be able to display the CyberTrust Seal of Assurance, it must meet one or more of the CyberTrust principles. The CyberTrust Seal of Assurance ensures that any Web site displaying it has met one or more standards established by CyberTrust.

The CyberTrust Seal of Assurance combines high standards for e-commerce activities with the requirement for a CyberTrust verification/audit. Together they build trust and confidence among consumers and businesses conducting business over the Internet. The entity has earned the right to display the Seal of Assurance with respect to the CyberTrust principle of:

Security:

The CyberTrust security principle requires an entity to meet high standards for the security of data transmitted over the Internet and stored on an e-commerce system. The independent verification/audit provides assurance that there are effective security policies, that the entity discloses its key security practices for electronic commerce, and that controls exist to ensure that these policies are followed. By committing to an independent verification/audit, the entity clearly demonstrates its commitment to data protection.



Appendix C. Construct items

Perceived trust

1. This vendor appears to be one who would keep promises and commitments.
2. I believe in the information that this vendor provides me.
3. I trust that this vendor keeps my best interests in mind.
4. The vendor is trustworthy.
5. I find that it is necessary to be cautious with this vendor (R).

R means the item is reversely scored.

All items are on a 7-point Likert-type scale.

Items measured in the paper: 1 = strongly disagree, …, 7 = strongly agree.

References

[1] J.C. Anderson, J.A. Narus, A model of distributor firm and manufacturer firm working partnership, Journal of Marketing 54 (1) (1990) 42–58.
[2] N. Anderson, Foundations of information integration theory, Academic Press, New York, 1981.
[3] S. Ba, A.B. Whinston, H. Zhang, The dynamics of the electronic market: an evolutionary game approach, Information Systems Frontiers 2 (1) (2000) 31–40.
[4] S. Ba, A.B. Whinston, H. Zhang, Building trust in online auction markets through an economic incentive mechanism, Decision Support Systems 35 (3) (2003) 273–286.
[5] BBB Accredited Business Seal 2009. http://us.bbb.org/WWWRoot/SitePage.aspx?site=113&id=5205182e-0e97-4f37-b37e-4c11c3e1e98a, last accessed on February 23, 2009.
[6] T. Bahmanziari, J.M. Pearson, L. Crosby, Is trust important in technology adoption? A policy capturing approach, Journal of Computer Information Systems 43 (4) (2003) 46–54.
[7] S. Balasubramanian, P. Konana, N.M. Menon, Customer satisfaction in virtual environments: a study of online investing, Management Science 49 (7) (2003) 871–889.
[8] A. Bhimani, Securing the commercial Internet, Communications of the ACM 39 (6) (June 1996) 29–31.
[9] K. Chiang, R.R. Dholakia, Factors driving consumer intention to shop online: an empirical investigation, Journal of Consumer Psychology 13 (1&2) (2003) 177–183.
[10] D.P. Cook, W. Luo, The role of third-party seals in building trust online, E-Service Journal 2 (3) (2003) 71–84.
[11] D.F. Cox, The sorting rule model of the consumer product evaluation process, in: D.F. Cox (Ed.), Risk Taking and Information Handling in Consumer Behavior, Division of Research, Graduate School of Business Administration, Harvard University, Boston, 1967.
[12] W.B. Dodds, K.B. Monroe, D. Grewal, Effects of price, brand, and store information on buyers' product evaluations, Journal of Marketing Research 28 (3) (1991) 307–319.
[13] P.M. Doney, J.P. Cannon, An examination of the nature of trust in buyer–seller relationships, Journal of Marketing 61 (2) (1997) 35–51.
[14] W. Ford, M.S. Baum, Secure Electronic Commerce, Prentice Hall, Inc., New Jersey, 1997.
[15] S. Ganesan, Determinants of long-term orientation in buyer–seller relationships, Journal of Marketing 58 (2) (1994) 1–19.
[16] D. Gefen, Customer loyalty in e-commerce, Journal of the Association for Information Systems 3 (1) (2002) 27–51.
[17] D. Gefen, E. Karahanna, D.W. Straub, Trust and TAM in online shopping: an integrated Model, MIS Quarterly 27 (1) (2003) 51–90.
[18] K. Griffin, P. Ladd, R. Whitehead, Internet commerce: security is still a concern, The Review of Accounting Information Systems 2 (1) (1997) 67–71.
[19] D.L. Hoffman, T.P. Novak, M. Peralta, Building consumer trust online, Communication of the ACM 42 (4) (1999) 80–85.
[20] X. Hu, Z. Lin, A.B. Whinston, H. Zhang, Hope or hype: on the viability of escrow services as trusted third parties in online auction environments, Information Systems Research 15 (3) (2004) 236–249.
[21] K.L. Hui, H.T. Hock, S.Y.T. Lee, The value of privacy assurance: an exploratory field experiment, MIS Quarterly 31 (1) (2007) 19–33.
[22] Internet Crime Complaint Center. IC3 2007 Internet crime report. Available: http://www.ic3.gov/media/annualreports.aspx. Last accessed on February 20, 2009.
[23] S. Jarvenpaa, L.N. Tractinsky, M. Vitale, Consumer trust in an Internet vendor, Information Technology and Management 1 (1&2) (2000) 45–71.

[24] D.J. Kim, D.L. Ferrin, H.R. Rao, A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents, Decision Support Systems 44 (2) (2008) 544–564.
[25] D.J. Kim, N. Sivasailam, H.R. Rao, Information assurance in B2C Websites for information goods/services, Electronic Markets 14 (4) (2004) 344–359.
[26] D.J. Kim, C. Steinfield, Y.J. Lai, Revisiting the role of web assurance seals in business-to-consumer electronic commerce, Decision Support Systems 44 (4) (2008) 1000–1015.
[27] K.M. Kimery, M. McCord, Third party assurances: the road to trust in online retailing, Proceedings of the 35th Hawaii International Conference on System Sciences, 2002.
[28] K.M. Kimery, M. McCord, Signal of trustworthiness in e-commerce: consumer understanding of third-party assurance seals, Journal of Electronic Commerce in Organizations 4 (4) (2006) 52–74.
[29] M. Koufaris, W. Hampton-Sosa, The development of initial trust in an online company by new customers, Information and Management 41 (3) (2004) 377–397.
[30] S.E. Kovar, K.G. Burke, B.R. Kovar, Consumer responses to the CPA WEBTRUST assurance, Journal of Information Systems 14 (1) (2000) 17–35.
[31] D. Maheswarn, S. Chaiken, Promoting systematic processing in low-motivation settings: effect of incongruent information on processing and judgments, Journal of Personality and Social Psychology 61 (1) (1991) 13–25.
[32] S.E. Maxwell, H.D. Delaney, Designing Experiments and Analyzing Data, Wadsworth Publishing Company, Belmont, CA, 1990.
[33] D.H. McKnight, V. Choudhury, C. Kacmar, The impact of initial consumer trust on intentions to transact with a Website: a trust building model, Journal of Strategic Information Systems 11 (3–4) (2002) 297–323.
[34] D.H. McKnight, L.L. Cummings, N.L. Chervany, Initial trust formation in new organizational relationships, Academy of Management Review 23 (3) (1998) 473–490.
[35] D.H. McKnight, C.J. Kacmar, V. Choudhury, Shifting factors and the ineffectiveness of third party assurance seals: a two-stage model of initial trust in a web business, Electronic Markets 14 (3) (2004) 252–266.
[36] A.D. Miyazaki, A. Fernandez, Consumer perception of privacy and security risks for online shopping, The Journal of Consumer Affairs 35 (1) (2001) 27–44.
[37] A.D. Miyazaki, D. Grewal, R.C. Goodstein, The effect of multiple extrinsic cues on quality perceptions: a matter of consistency, Journal of Consumer Research 32 (1) (2005) 146–153.
[38] T. Moores, Do consumers understand the role of privacy seals in e-commerce? Communications of the ACM 48 (3) (2005) 86–91.
[39] T.T. Moores, G. Dhillon, Do privacy seals in e-commerce really work? Communications of the ACM 46 (12) (2003) 265–271.
[40] C. Moorman, R. Deshpande, G. Zaltman, Factors affecting trust in market research relationships, Journal of Marketing 57 (1) (1993) 81–101.
[41] R.M. Morgan, S.D. Hunt, The commitment-trust theory of relationship marketing, Journal of Marketing 58 (3) (1994) 20–38.
[42] A. Noteberg, E. Christiaanse, P. Wallage, Consumer trust in electronic channels: the impact of electronic commerce assurance on consumers' purchasing likelihood and risk perceptions, e-Service Journal 2 (2) (2003) 46–67.
[43] J.C. Nunnally, Psychometric Theory, 2nd ed. McGraw-Hill Book Company, New York, 1978.
[44] M.D. Odom, A. Kumar, L. Saunders, Web assurance seals: how and why they influence consumers' decisions, Journal of Information Systems 16 (2) (2002) 231–250.
[45] D. O'Keefe, Message properties, mediating states, and manipulation checks: claims, evidences, and data analysis in experimental persuasive message effects research, Communication Theory 13 (3) (2003) 251–274.
[46] J. C. Olson, Cue utilization in the quality perception process: a cognitive model and an empirical test, doctoral dissertation, Purdue University, 1972.
[47] J.C. Olson, J. Jacoby, Cue utilization in the quality perception process, in: M. Venkatesam (Ed.), Proceedings of 3rd Annual Conference, Association for Consumer Research, Chicago, 1973, pp. 167–179.
[48] R.H. Pennington, D. Wilcox, V. Grover, The role of system trust in business-to-consumer transactions, Journal of Management Information system 20 (3) (2003) 197–226.
[49] B.C. Perdue, J.O. Summers, Checking the success of manipulations in marketing experiments, Journal of Marketing Research 23 (1986) 317–326.
[50] D. Purohit, J. Srivastava, Effects of manufacturer reputation, retailer reputation, and product warranty on consumer judgments of product quality: a cue diagnosticity framework, Journal of Consumer Psychology 10 (3) (2001) 123–134.
[51] A.R. Rao, K.B. Monroe, The moderating effect of prior knowledge on cue utilization in product evaluations, Journal of Consumer Research 15 (2) (1988) 253–264.
[52] P.S. Richardson, A.S. Dick, A.K. Jain, Extrinsic and intrinsic cue effects on perceptions of vendor brand quality, Journal of Marketing 58 (4) (1994) 28–36.
[53] N.J. Rifon, R. LaRose, S.M. Choi, Your privacy is sealed: effects of web privacy seals on trust and personal disclosures, Journal of Consumer Affairs 39 (2) (2005) 339–362.
[54] K.J. Stewart, Trust transfer on the World Wide Web, Organization Science 14 (1) (2003) 5–17.
[55] Trust Guard Certified Seal 2009. http://www.trust-guard.com/Trust-Guard-Certified-Seal-p/tg_certified_indiv.htm, last accessed on February 23, 2009.
[56] U.S. Census Bureau, Quarterly retail e-commerce sales: 4rd quarter 2008. Available: http://www.census.gov/mrts/www/data/html/08Q4.html, last accessed on February 25, 2009.
[57] D. Van den Poel, J. Leunis, Consumer acceptance of the internet as a channel of distribution, Journal of Business Research 45 (3) (1999) 249–256.
[58] S. Wang, S.E. Beatty, W. Foxx, Signaling the trustworthiness of small online retailers, Journal of Interactive Marketing 18 (1) (2004) 53–69.

Xiaorui Hu is an Associate Professor of Decision Sciences and Information Technology Management at the John Cook School of Business, Saint Louis University. She received her Ph.D. in Economics from the University of Texas at Austin. Her research focuses on trust related issues in electronic commerce, culture impact on international business, and ethical issues in Internet age. She has published in *Information Systems Research, Decision Support Systems, IEEE Computer, Journal of Organizational Computing and Electronic Commerce*, and other academic journals.

Guohua Wu is an Assistant Professor of Communications at California State University, Fullerton. He received his Ph.D. in Communication from the University of Texas at Austin. His research interests focus on the role of interactivity in online consumer's attitude and trust formation. His articles have appeared in *International Journal of Advertising, Journal of Consumer Marketing, Journal of Interactive Advertising, Journal of Current Issues and Research in Advertising, and Journal of Computer-mediated Communication*.

Yuhong Wu received her Ph.D. in marketing from the University of Texas at Austin. Her research interests lie in the areas of Internet marketing and e-commerce, strategies in network market, and new product development and management. She has published in *Journal of Marketing* and other academic journals.

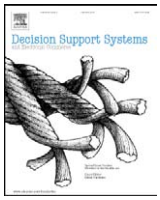
Han Zhang is an Associate Professor of Information Technology Management at the College of Management, Georgia Institute of Technology. He received his Ph.D. in Information Systems from the University of Texas at Austin. His research focuses on online trust and reputation related issues, trusted third parties or intermediaries, the evolution of electronic markets, and online payment methods. He has published in *Information Systems Research, Journal of Management Information Systems, Decision Support Systems*, and other academic journals.

Decision Support Systems 49 (2010) 250

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss



Erratum

Erratum to "The effects of third-party web assurance seals on consumers' initial trust in online vendors: A functional perspective" [Decision Support Systems Volume (48/2) 407–418]

Xiaorui Hu [a,*], Guohua Wu [b], Yuhong Wu [c], Han Zhang [d]

[a] *Saint Louis University, United States*
[b] *California State University, Fullerton, United States*
[c] *Houston, TX, United States*
[d] *Georgia Institute of Technology, United States*

The publisher regrets that when the above paper was published we omitted to include the information that the authors are listed alphabetically. The publisher would like to apologise for any inconvenience this may have caused to the authors of this article and readers of the journal.

DOI of original article: 10.1016/j.dss.2009.10.004.
* Corresponding author.
E-mail addresses: hux2@slu.edu (X. Hu), mwu@fullerton.edu (G. Wu), yuhong_ut@yahoo.com (Y. Wu), han.zhang@mgt.gatech.edu (H. Zhang).

0167-9236/$ – see front matter
doi:10.1016/j.dss.2010.01.001