TRUSTMARKS AS INTERNET CERTIFICATIONS: AN INVESTIGATION OF SOURCE INFLUENCES

K. Damon Aiken, California State University, Chico
kaiken@csuchico.edu

ABSTRACT

This study provides a foundational investigation of the source influences of internet "trustmarks" (i.e., any third-party mark, logo, picture, or symbol, presented in an effort to dispel consumers' concerns about security and privacy). An experiment utilized three identical marks, but it manipulated the certifying source as coming from either the government, industry experts, or consumer reviews (along with a control condition). Results show that the governmental trustmark was most influential in building cognitive and affective trust. Additionally, male subjects were generally more trusting than female subjects.

INTRODUCTION

For many years now, the notion of trust has been thoroughly studied by researchers in the fields of psychology, sociology, economics, and business (see Swan, Bowers, & Richardson, 1999 for a meta-analysis). Whether trust is perceived as a cognitively-developed attitude (Doney & Cannon, 1997), an innate emotion (Luhman, 1979), a calculated belief (Williamson, 1993), or a required social force allowing us freedom from prediction and confidence in interactions (Lewis & Weigert, 1985), the existence of trust is notoriously important to business and social exchange. Trust is seen as the very foundation upon which relationship marketing is built (Berry, 1995). Even within the relatively new and ever-changing world of the Internet, researchers have noted that *e*commerce requires a base level of trust between the consumer and the organization (Grabner-Krauter & Kaluscha, 2003).

Consequently, an interesting communications phenomenon has emerged. Internet firms must send/post computer-mediated signals (i.e., actions that parties take to reveal their true types, Kirmani & Rao, 2000) to get across critical information to potential consumers. In order to signal trustworthiness, internet-based firms have begun to seek out and post *e*commerce-specific certifications from objective third parties, effectively renting the reputation of another. For example, the VeriSign company now processes over 650 million views daily on over 100,000 websites worldwide (*www.verisign.com*). The TRUST*e* company claims to be the most recognized Internet seal in the world with more than 75% of unique Internet users (amongst the over two billion – Internet World Stats 2011) exposed to TRUST*e* certified websites each month (*www.truste.com*). Not to be outdone, the Better Business Bureau boldly states, "Almost 90% of online shoppers would feel more confident shopping on a site that displays the BBBOnLine

Seal" (*www.bbbonline.org*). Apparently, internet businesses have taken notice that lack of trust, along with the associated privacy and security concerns, is often the most frequently cited reason for consumers not purchasing from *e*tailers (Benassi, 1999; Hine & Eve, 1998; Sheehan & Hoy, 2000; Sipior, Ward, & Mendoza, 2011). Thus, firms are attempting to build trust through various seals, certifications, "authenticators" (Rust, Kannan, & Peng, 2002), and trustmarks (Aiken, Osland, Liu, & Mackoy, 2003).

Given this well-justified proliferation of third-party certifications amongst *e*tailers, the concept of trust transference (Doney & Cannon, 1997; Milliman & Fugate, 1988) plays a very important part in internet marketing. The internet is a communications context wherein information asymmetry abounds. Offered relatively few informational cues, presented mostly in visual written and iconographic forms, internet consumers must frequently ascribe notions of trustworthiness from outside-source signals. Some of these outside-source signals have aptly taken on the designation of "trustmarks" (Aiken, et al., 2003). Trustmarks have been defined as any third-party mark, logo, picture, or symbol, presented in an effort to dispel consumers' concerns about internet security and privacy and, therefore, to increase firm-specific trust levels (Aiken, Liu, Mackoy, & Osland, 2004). A trustmark is designed to communicate trustworthiness through behavioral insinuations of capability, rational suggestions of credibility, and emotional implications of benevolence and integrity. Usually, an internet firm must license the trustmark from some third-party – compensating the party through both an upfront fee and a monthly payment. The issuing firm investigates the company, its internet security methods and specific *e*commerce practices, and then authorizes the licensor to post the mark on its website. Consumers are then assured that there are certified security, privacy and disclosure standards for the use and access of information that they provide to the organization (Russell & Lane, 2002).

Marketing researchers have learned that context-specific trustmarks are effective (Aiken & Boush, 2006); however, the field has yet to more deeply investigate many of the complex signal-based communications processes surrounding trustmarks. Thus, the current work has two main objectives. First, the study serves as a preliminary investigation into the process of trust development through the use of trustmarks. Second, the study specifically explores the impact of source influences of trustmarks in early stages of trust transference. A between-subjects experiment manipulates only the source characteristics of stimuli so as to come from: (1) a governmental source; (2) consumer reviews; and (3) an objective, expert third-party source (along with a control condition). The sections below discuss extant literature, share the study's method and results, and discuss findings and managerial implications.

TRUST IN A COMPUTER-MEDIATED ENVIRONMENT

Prior to the explosion of the internet as an all-in-one distribution, promotion, and marketing tool, researchers recognized the multitude of situational factors and noted that trust is both target- and context-specific (Aiken, 1999; Johnson-George & Swap, 1982; Schurr & Ozanne, 1985). Previous research has studied internet trust at both the firm-specific level (Jarvenpaa &

Tractinsky, 1999; Luo, 2002; Shankar, Urban, & Sultan, 2002; Sultan et al., 2002; Yoon, 2002), the community-level (Blanchard, Welbourne, & Boughton, 2011), as well as the broader, more macro-environmental context. For instance, Mutz (2005) evaluates *e*commerce in terms of general social trust. Moreover, while Grabner-Krauter and Kaluscha (2003) speak of system trust, Walczuch and Lundgren (2004) describe institution-based trust in *e*comnmerce in general. Chen and Dhillon (2003) propose three primary dimensions of *generalized* Internet trust, namely: competence, integrity, and benevolence.

An ever-expanding subset of the business and marketing literature concentrates on how the concept of trust is unique in a computer-mediated environment (Handy, 1995; Hine & Eve, 1998; Jarvenpaa & Tractinsky, 1999; Koehn, 2003; McKnight & Chervany, 2002). In the context of the Internet, buyers and sellers exist in a computer-mediated *marketspace* wherein issues are not resolved face-to-face; but rather, distant users attempt to communicate through a globally elaborate "web" of electronics hardware and software (Dugal & Roy, 2000; Hoffman, Novak, & Perralta, 1999a). Internet firms and *infomediaries* are positioned between producers and the growing throng of *e*consumers (Parasuraman & Zinkhan, 2002). Communications and transactions occur electronically, thereby increasing risks for online consumers and placing a heavy communications burden on sellers whose website effectiveness is affected by a variety of design characteristics (Geissler, Zinkhan, & Watson, 2001). Trust in the Internet is further complicated by the fact that developmental attributes of online trust are influenced by the shopping trip's specific purpose (Reibstein, 2002).

Contemporary definitions of trust in the internet reflect new-found consumer apprehensions. Overcoming perceptions of uncertainty has linked trust to the diffusion and acceptance of *e*commerce in general (Grabner-Kraeuter, 2002; Shankar, Urban, & Sultan, 2002). Internet consumers worry about everything from excessive spam e-mails and intrusive cookie files, to costly credit card fraud and perilous identity theft. Milne and Boza (1999) define trust in terms of this largely affective privacy element, noting the expectancy of an internet consumer to rely on marketers to treat personal information fairly. Thus, issues of risk, reliability, privacy, security and control of information emerge as key variables in internet trust development (Bhatnagar & Ghose, 2004; McCole, Ramsey, & Williams, 2010). These issues dominate firm-specific or website-specific trust research (e.g., Garbarino & Strahilivitz, 2004; Sultan et al., 2002; Yoon, 2002).

In this way, society in the information age (Glazer, 1991) seems to have developed a new form of *contextual* trust - a form of trust that is characterized by the unique representations of *e*consumers and virtual firms as encoded, transmitted, and decoded through an electronics-driven computer-mediated environment (Aiken & Boush, 2006). Contextual trust appears to be affected by the communications-media involved, the unusual shopping environment, and the transaction-specific risks and rewards. Every aspect of internet consumption, including communications, transactions, and even terms of delivery, is moderated by an omnipresent generalized trust of the media context itself (Aiken et al., 2007). Further, this form of contextual Internet trust

encompasses issues of risk, reliability, privacy, and security, as well as perceptions related to control of information (Rust, Kannan, & Peng, 2002; Strauss & Frost, 1999).

Overcoming the concern for privacy is a major building block for trust development in the internet (Hine & Eve, 1998; Benassi, 1999). Researchers have observed that privacy is a multidimensional concept and plays a critical role in fear of purchasing online (Hine & Eve, 1998; Sheehan & Hoy, 2000). This concern for privacy likely derives from fear of the unknown (Hoffman, Novak, & Peralta, 1999b). In as much as trust requires a cognitive and affective leap of faith (a movement beyond calculative prediction – see Williamson, 1993), trust in the internet implies, to some extent, behaviorally overcoming a concern for privacy. To take action in the face of risk is to engage in trusting behavior (Moorman, Zaltman, & Deshpandé, 1992; Schurr & Ozanne, 1985). Such action appears as a cognitive abstraction of trust - an imperfect attempt to rationally estimate the incalculable possibilities of risks and rewards (Aiken, Liu, Mackoy, & Osland, 2004).

Moreover, trust in the internet involves unique issues of control. In the off-line world consumers think nothing of giving their phone numbers or home addresses to seemingly disinterested cashiers and store managers. However, online consumers often cite feelings of helplessness and fear while shopping on the internet (Hine & Eve, 1998). *E*consumers often desire complete control over their personal information, control over the actions of a web vendor, and control over the Internet site. Managing the actions of an Internet firm affects consumer perceptions of privacy and security (Bhatnagar & Ghose, 2004; Hoffman, Novak, & Peralta, 1999b). Thus, internet consumers carefully guard their personal information.

Finally, internet trust has been noted to carry with it unusual behavioral burdens. That is, internet behaviors and behavioral intentions are consistently judged by *e*consumers and potential *e*consumers alike. A firm's resources and abilities are meticulously judged, discussed in chat rooms, and rated by all types of consumers and groups. Trust in an internet context, then, largely develops through keeping behavioral promises. Accordingly, an evolving sense of "Darwinian trust" emerges as the new essence of online commerce (Alsop, 1999). Koehn (2003) speaks of the related concepts of *calculative trust* (parties reviewing another's history of keeping promises), as well as the *knowledge-based trust* (that emerges when two parties are familiar with each other and interact frequently). Past behaviors lead to greater trust. And, in an internet context in which both inexperience and uncertainty abound, any and all concrete behavioral assessments are applied in the trust development process. Thus, third-party certifications, ratings, reviews, and trustmarks take on greater weight through the process of trust transference (Aiken, 1999; Aiken, et al., 2004; Doney & Cannon, 1997; Miliman & Fugate, 1988).

Trust Development through Transference

The internet has drastically changed the acquisition, processing, and management of information (Biswas & Biswas, 2004). Transference serves a communicative function in information processing. In this sense, it is a reasonable evolved consumer heuristic to transfer feelings and cognitions from a trusted proof source to another person or group with which the consumer has little or no experience. This communicative "short cut" makes even more sense in a computer-mediated context wherein information asymmetry abounds.

Thus, in an attempt to answer the fundamental question, "How does trust develop in a business relationship?" many authors have recognized myriad antecedents (Doney & Cannon, 1997; Ganesan, 1994; McAllister, 1995; Morgan & Hunt, 1994; Schurr & Ozanne, 1985; Swan, Bowers, & Richardson, 1999). Antecedents are generally viewed as contributors of the process that brings a trustor away from a state of either neutrality or distrust. The process of trust development relies on the formation of expectations (under the influence of individual perception) about the motives and behaviors of a trustee. In order to better understand the complexities of interpersonal trust development, Doney and Cannon (1997) proposed "Five Cognitive Processes." One was labeled the *transference process* wherein researchers noted that trust can develop by attaining a third party's definition or opinion of another as trustworthy. This suggests that trust can be transferred from one trusted source to another person or group with which the trustor has little or no experience. These processes are an acknowledgment that something happens between the apperception of an antecedent and the emergence of trust.

Trustmarks as Internet Signals

The concept of signaling theory is derived from a widely accepted economic idea that parties involved in a transaction will have varying levels of information (Bergen, Dutta, & Walker, 1992; Mishra, Heide, & Cort, 1998; Rao & Monroe, 1996). This potential discrepancy of information has implications for possible transactions and relationships between the parties (Bagwell & Riordan, 1991; Boulding & Kirmani, 1993). Kirmani and Rao (2000) further explain signaling theory and its complications by stating that, "When one party lacks information that the other party has, the first party may make inferences from the information provided by the second party, and this inference should play a role in the information the second party chooses to provide" (p. 67). By choosing what to project to outsiders, the information becomes a signal. Lastly, signaling theory posits that a rational consumer expects a firm to honor the implicit commitment conveyed by a signal, since not honoring a promise is viewed as economic suicide for a company (Bagwell & Riordan, 1991; Boulding & Kirmani, 1993).

In the context of the Internet, signals may be of utmost importance in terms of consumer diagnostics (Biswas & Biswas, 2004). Marketers are faced with the difficult task of truly understanding their customer base. Only then can marketers choose the most appropriate signal

to send an effective message, reducing customers' apprehensions and thereby declaring the website trustworthy. Furthermore, this signal must be placed in the most advantageous place on the web page, making it easily readable and convenient for customers to see, but not so forthcoming that it actually increases uneasiness among the customer base (it is conceivable that consumers might call into question the need for a firm to send such a strong signal). Aiken et al. (2004) present a suitable categorization of 20 possible Internet signals (e.g., trustmarks, consumer reviews, chat rooms, banner ads, online coupons, return policies, warranties, translations of sites, etc.).

Finally, previous studies have shown that choosing an appropriate third-party is critical to how potential consumers will react to the trustmark. That is, the third-party must be seen as credible in order to be effective (Russell & Lane, 2002). Garbarino and Strahilevitz (2004) found that site recommendations (from friends) lead to both greater reductions in perceived risk and also stronger purchase intentions. A better understanding of the influences of source characteristics of trustmarks would have a great impact on the effectiveness of the mark a company utilizes.

METHOD

A between-subjects experiment attempted to measure trustmark source influences on firm-specific trust utilizing four conditions (inclusive of a control condition). Since the research was exploratory there were no a priori hypotheses. A convenience sample of 400 subjects was taken from a large northwestern university. The sample consisted of approximately 90% undergraduate students and 10% graduate students from across the school's four major colleges (thus generating subjects from a wide variety of study disciplines). While 21 of the surveys were deemed unusable, an additional 21 surveys came from self-identified international students and were set aside for future comparative analyses. The remaining 358 usable questionnaires contained 168 female (46.9%) and 189 male (52.9%) subjects.

Data collection took place in classroom settings rather than over the internet in order to increase response rates and to increase subjects' involvement levels. The paper-and-pencil questionnaire consisted of three parts. Nearly all of the variables were measured using seven-point Likert-type scales. Part One provided an introduction to the study and inquired about generalized Internet commerce trust (GICT). The scale was adapted from Aiken et al. (2007) and measured the five dimensions of GICT.

Part Two opened with another short introduction, written in a font size three times that of the rest of the questionnaire. The short paragraph provided further introduction to the stimuli and implored subjects to pay special attention to the website they were about to see. They were asked to "spend one-two minutes carefully examining all aspects of the following web page." Next, one of four possible experimental stimuli were presented in the form of a screen print from a mock website. The site posed as a new electronics superstore and the specific page highlighted a digital

camera for sale. Three different internet trustmarks were presented in the lower right corner of each website. These trustmarks were designed by a graphic artist so as to look realistic but not especially familiar or recognizable as any company that subjects would have seen before. The main design element was a lock -- meant to instill a sense of security and protection. Above the graphic was the name "SiteSecure." The slogan of the mock company was "Keeping Consumers Safe on the Internet," and was shown below the lock and above the name of the firm in all three experimental conditions. The trustmarks only differed in terms of the identification of the certifying source at the bottom of the mark. Phrases at the bottoms of the trustmarks were: (1) "Reviewed and Certified by Customers Like You;" (2) "PC Magazine - Editors' Choice;" and (3) "The Bureau of Consumer Protection (A Division of the Federal Government)," with the latter two having green text above the phrase which read "Certified By." This was not placed on the Customer review condition in order to avoid redundancy. Additionally, there was a control condition, picturing all elements of the company, the website, as well as the camera and its functions, without any trustmark. Exposure to experimental conditions was randomly assigned.

Part Three of the questionnaire contained variables adapted from Aiken and Boush's (2006) measurement of firm-specific trust (FST). Here, variables attempted to measure the affective, behavioral, and cognitive elements of trust in the experimental website. After the firm-specific trust questions, subjects were asked several demographic and Internet-usage questions.

RESULTS

Generalized Internet Commerce Trust Results

Cumulatively, the GICT scale yielded a Cronbach's alpha of 0.68. While a principle components factor analysis validated the same five dimensions found previously by Aiken et al. (2007), separate analyses of each component is beyond the scope of this paper. Thus, an aggregated GICT mean was calculated by averaging responses to Part One of the survey. The mean for the sample was 3.91 on a seven point scale. This relatively low overall trust of the Internet, in general, is consistent with previous research noting that people are still hesitant to trust web information (Gosling, 2004).

After running frequencies and placing subjects into two relatively equal sized GICT groups, a set of oneway ANOVA and t-tests were run. First, with respective means of 3.53 and 4.51, it was not surprising that low trusters had significantly lower GITC scores than high trusters ($t = 22.8$, $p < .01$). Additionally, across gender groups, the data showed that men were more trusting, in terms of generalized Internet commerce, than women (male mean = 4.12, female mean = 3.85; $t = 4.05$, $p < .01$).

Second, after blocking on those subjects displaying high levels of GICT (and then low levels of GICT), an ANOVA revealed that high GITC subjects exposed to the government-sourced trustmark displayed significantly higher firm-specific trust means ($F = 4.44$, $p < .01$). Furthermore, in post hoc tests the government condition had significantly higher firm-specific trust means compared to the both the control condition ($p < .01$) and the independent experts condition ($p < .05$). High GITC subjects seemed to be more influenced by the government-sourced trustmark. Low GITC subjects were not swayed by exposure to the different conditions.

Third, an ANOVA found significant differences between GITC groups and their firm-specific trust scores (after controlling for exposure to experimental stimuli). Thus, generalized Internet trust was determined to be a significant moderating variable between the trustmark condition and firm-specific trust ($F = 11.02$, $p < .01$) as well as the three base components of firm-specific trust. Lastly, the GICT means across Internet usage groups and Internet purchasing groups failed to show statistical significance. Essentially, regardless of the number of hours spent on the Internet, or the number of items purchased through the Internet, subjects' levels of GICT were quite similar.

Firm-Specific Trust Results

Firm-specific trust (FST) was measured according to the three foundational components (affective, behavioral, and cognitive) recognized by so many previous researchers (see Aiken & Boush, 2006; Doney & Cannon, 1997; Ganesan, 1994; Johnson & Grayson, 2005; Lewis & Weigert, 1985). Means were calculated for each component and in total. Cronbach's alpha scores were .934 for total FST, .720 for affective FST, .925 for behavioral FST, and .921 for cognitive FST. It is interesting to note the striking differences in means between behavioral elements of trust and other aspects of trust. Subjects were quite distrustful of the experimental firm in terms of providing their email and home addresses, their phone numbers, and their "personal demographic information."

A set of *ANOVA* and t-tests were utilized to investigate differences in FST means. When FST means were analyzed across experimental conditions, the means of the group exposed to the governmental source were consistently higher than that of subjects in the other three groups. The differences were statistically significant for the combined measure of FST ($F = 4.22$, $p < .01$). Further analyses showed that the government-sourced trustmark favorably influenced affective trust ($F = 5.05$, $p < .01$) as well as cognitive trust ($F = 4.46$, $p < .01$), but it did not have an effect on the behavioral FST component. Post hoc tests utilizing Tukey's HSD multiple comparisons further reinforced the power of the government-sourced trustmark.

TABLE 1: FIRM-SPECIFIC TRUST BY TRUSTMARK SOURCE CONDITION *

Source Condition	Affective Trust Means	Behavioral Trust Means	Cognitive Trust Means	
Government Certified (n = 90)	4.16 (s = .93)	3.39 (s = 1.41)	4.14 (s = 1.10)	3.89 (s = 1.02)
Consumer Certified (n = 90)	3.92 (s = .92)	3.17 (s = 1.32)	3.99 (s = 1.16)	3.70 (s = .99)
Industry Expert Certified (n = 91)	3.83 (s = 1.07)	3.22 (s = 1.58)	3.72 (s = 1.29)	3.59 (s = 1.21)
Control Condition (n = 87)	3.61 (s = .85)	2.85 (s = 1.36)	3.55 (s = 1.16)	3.34 (s = .99)
ANOVA results	F = 5.05 p < .01	F = 2.17 p < .09	F = 4.46 p < .01	F = 4.22 p < .01

* 7-point scale

Testing FST levels according to internet usage groups (high, medium, and low – as broken down according to self-reported numbers of hours spent on the internet) showed practically no mean differences. Furthermore, testing FST levels according to internet shopping groups (low, medium, and high relative to the self-reported number of annual internet purchases) revealed practically no differences in FST means. In other words, subjects who were heavy internet users were not differentially influenced by the source characteristics of the trustmarks.

Finally, the sample showed significant FST differences across gender groups. Just as noted above in terms of GICT, men showed higher trust levels than women at the firm-specific level. A set of t-tests revealed that, in aggregate of all experimental conditions, men showed significantly higher levels of FST (3.82 compared to 3.42, $t = 2.83$, $p < .01$) as well as the corresponding foundational bases of FST. However, analyzing each experimental condition separately, we see that this gender distinction was largely driven by significant differences in the consumer-sourced condition and the control condition. That is, male subjects responded more positively to the consumer-sourced condition and were less distrustful of the control condition. The pattern was inconsistent across the industry expert condition and gender means were nearly equal in the government-sourced condition.

DISCUSSION

The overarching purpose of this study was to explore the source influences of internet trustmarks. After careful analyses, several conclusions can be drawn with confidence. First, with respect to firm-specific trust, the results revealed that amongst the three sources the government-sourced trustmark was the most influential. Given the US tendency to rate high on individualism (vs. collectivism) according to Hofstede (1980), one might have expected the Industry Experts source to induce the highest levels of FST. Anecdotally, one might reason that this result was also surprising given a growing distrust of the US government in the wake of bank scandals, bailouts, etc. Yet, at least amongst college students, it appears that federal agencies instill greater perceptions of security than do other sources. Perhaps this age cohort views federal certifications as highly credible. Or, perhaps college students, for the most part extremely technologically savvy, understand the ease of posting reviews (either from consumers or industry experts) and so they somehow discount the informational value of these sources.

Second, our findings reveal that the behavioral component of trust is still not usually higher than the affective or cognitive components of FST. Further, consumers' behavioral trust is not significantly influenced by trustmarks. This study found that the sources of trustmarks did not have any influence on behavioral trust. So, although it might appear on the surface that college students are exceedingly comfortable giving out personal information (e.g., email addresses, phone numbers, and even their home addresses) over the internet, they are actually much more generous and optimistic (or perhaps less cautious and restrictive) in their affective and cognitive judgments. It is interesting to note that, behaviorally speaking, a significant number of people regularly give false personal information over the Internet (Hoffman, Novak, & Perralta, 1999a).

Third, the data show that men not only have higher levels of generalized Internet commerce trust, but that they also (oftentimes) are more trusting at the firm-specific level compared to women. These results are consistent with previous findings that women are more concerned with privacy, security, and risk (Sheehan & Hoy, 2000). Still, the aggregated GICT mean was only 3.81 (below the midpoint of the 7-point scale). This moderately low number is surprising, given the longstanding emphasis on security in *e*commerce. Additionally, many Internet users are protected through the use of anti-virus software, malware, as well as fraud and identity theft guarantees that did not exist a decade ago. Still, even with advanced technology, this study provides evidence that consumers are quite reluctant to trust on the Internet.

Lastly, from the purchasing behavior data gathered, medium purchasers tend to have the highest GICT. At first glance, this finding seems surprising because the mid-level does not have the most experience with online purchasing. However, it may be that the medium purchasers have the highest GICT because they have had fewer negative experiences. Perhaps heavy purchasers are more likely to have experienced theft or fraud through their many Internet transactions. The low purchasing group also included respondents who had never made a purchase online. These include the skeptics, who may have never trusted the Internet.

LIMITATIONS AND FUTURE RESEARCH

This study suffers from many of the most common plights of academic research. First, although this study would ideally be generalized to the entire population of Internet users, the sample was derived purely from college students in roughly the same age range. While one might argue that students go through the same cognitive processes of inference making and trust transference as the general population, there still may be something idiosyncratic about this group with regards to their interpretations of internet signals. Future studies should take care to include wider demographic and geographic ranges.

Second, the stimuli were presented on a mock website, which displayed a fabricated trustmark, and the data were collected in a lab-type setting. While this was done to eliminate any potential biases, to control for external confounds, and to heighten involvement levels of respondents, the experiment may have suffered from perceived artificiality. This may have reduced trust levels across the board, due to fear of the unknown or a general lack of realism. Steps to increase the realism (i.e., using an existing trustmark, a real internet firm, and collecting data over the internet) would likely increase the validity of the study. Still, future studies would have to take measures to ensure against biases that might stem from previous interactions and perhaps well-formed attitudes about a test company, brand, or existing trustmark. Regardless, the complex and interesting sub-field of internet commerce and communication signaling through trustmarks requires further exploration and empirical validation.

REFERENCES

Aiken, D. (1999). Explorations in Interpersonal Trust Development: The Trust Curve, in *Enhancing Knowledge Development in Marketing*, Eds. S.P. Brown and D. Subharshan, American Marketing Association: Chicago, 10, 59-67.

Aiken, D. & Boush, D. (2006). Trustmarks, Objective-Source Ratings, and Implied Investments in Advertising: Investigating Online Trust and the Context-Specific Nature of Internet Signals, *Journal of the Academy of Marketing Science*, 34(3), 308-323.

Aiken, D., Liu, B., Mackoy, R., & Osland, G. (2004). Building Internet Trust: Signaling Through Trustmarks, *International Journal of Internet Marketing and Advertising*, 1(3), 1-17.

Aiken, D., Mackoy, R., Liu, B., Fetter, R. & Osland, G. (2007). Dimensions of Internet Trust, *Journal of Internet Commerce*, 6(4), 1-25.

Aiken, D., Osland, G., Liu, B., & Mackoy, R. (2003). Developing Internet Consumer Trust: Exploring Trustmarks as Third-Party Signals, in *Marketing Theory and Applications*, Eds. G.R. Henderson and M.C. Moore. Chicago: American Marketing Association, 14, 145-146.

Alsop, S. (1999). You Can Trust Me On This – Really, *Fortune*, 139(5), 175-176.

Bagwell, K., & Riordan, M. (1991). High and Declining Prices Signal Product Quality, *American Economic Review*, 81(March), 224-239.

BBBonline (2011). http://www.bbbonline.org, accessed June, 2011.

Benassi, P. (1999). Truste: An Online Privacy Seal Program, *Communications of the ACM*, 42(2), 56-59.

Bergen, M, Dutta, S., & Walker, O. (1992). Agency Relationships in Marketing: A Review of the Implications and Applications of Agency and Related Theories, *Journal of Marketing,* 56(2), 1-24.

Berry, L. L. (1995), Relationship Marketing of Services – Growing Interest, Emerging Perspectives, *Journal of the Academy of Marketing Science*, 23(4), 236-245.

Bhatnagar, A., & Ghose, S. (2004). Segmenting Consumers Based on the Benefits and Risks of Internet Shopping, *Journal of Business Research*, 57(12), 1352-1360.

Biswas, D. & Biswas, A. (2004). The Diagnostic Role of Signals in the Context of Perceived Risks in Online Shopping: Do Signals Matter More on the Web? *Journal of Interactive Marketing*, 18(3), 30-45.

Blanchard, A., Welbourne, J., & Boughton, M. (2011). A Model of Online Trust: The Mediating Role of Norms and Sense of Virtual Community, *Information, Community, and Society*, 14(1), 76-106.

Boulding, W. & Kirmani, A. (1993). A Consumer-Side Experimental Examination of Signaling Theory: Do Consumers Perceive Warranties as Signals of Quality? *Journal of Consumer Research*, 19(2), 111-123.

Chen, S.C. & Dhillon, G.S. (2003). Interpreting Dimensions of Consumer Trust, *Information Technology and Management*, 4 (2-3), 303-318.

Chu, W. & Chu, W. (1994). Signaling Quality by Selling Through a Reputable Retailer: An Example of Renting the Reputation of Another Agent, *Marketing Science,* 13(Spring), 177-189.

Doney, P. & Cannon, J.P. (1997). An Examination of the Nature of Trust in Buyer Seller Relationships, *Journal of Marketing*, 61(April), 35-51.

Dugal, S. S. & Roy, M. H. (2000). A Management Guide to the Creation of Product and Service Images Marketspace. *International Journal of Management*, 17(3), 349-354.

Garbarino, E. & Strahilevitz, M. (2004). Gender Differences in the Perceived Risk of Buying Online and the Effects of Receiving a Cite Recommendation, *Journal of Business Research*, 57(7), 768-775.

Ganesan, S. (1994). Determinants of Long-Term Orientation in Buyer-Seller Relationships, *Journal of Marketing*, 58(April), 1-19.

Geissler, G., Zinkhan, G., & Watson, R.T. (2001). Web Home Page Complexity and Communication Effectiveness, *Journal of the Association for Information Systems*, 2(April), 1-46.

Glazer, R. (1991). Marketing in an Information-Intensive Environment: Strategic Implications of Knowledge as an Asset, *Journal of Marketing*, 55(Oct.), 1-19.

Gosling, S. (2004). Should We Trust Web-Based Studies? A Comparative Analysis of Six Preconceptions About Internet Questionnaires, *American Psychologist*, 59(2), 93-104.

Grabner-Kraeuter, S. (2002). The Role of Consumers' Trust in Online Shopping. *Journal of Business Ethics*, 39(1-2), 43-50.

Grabner-Kraeuter, S. & Kaluscha, E. (2003). Empirical Research in On-Line Trust: A Review and Critical Assessment, *International Journal of Human-Computer Studies*, 58(6), 783-812.

Handy, C. (1995). Trust and the Virtual Organization, *Harvard Business Review*, 73(3), 40-50.

Hine, C. & Eve, J. (1998). Privacy in the Marketplace, *The Information Society*, 4(4), 253-262.

Hoffman, D., Novak, T., & Peralta, M. (1999a). Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web, *The Information Society*, 15, 129-139.

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

Hofstede, G. (1980). *Culture's Consequences, International Differences in Work-Related Values,* Sage Publications: Thousand Oaks.

Internet World Stats (2011). Internet Usage Statistics. The Internet Big Picture. World Internet Population Stats, http://www.internetworldstats.com/stats.htm, Accessed May 2011.

Jarvenpaa, S. & Tractinsky, N. (1999). Consumer Trust in an Internet Store: A Cross-Cultural Validation, *Journal of Computer-Mediated Communications*, 15(2), 1-35.

Johnson, D. & Grayson, K. (2005). Cognitive and Affective Trust in Service Relationships, *Journal of Business Research*, 58(4), 500-550.

Johnson-George, C. & Swap, W. C. (1982). Measurement of Specific Interpersonal Trust: Construction and Validation of a Scale to Assess Trust in a Specific Other, *Journal of Personality and Social Psychology*, 43(6), 1306-1317.

Kirmani, A. & Rao, A. (2000). No Pain, No Gain: A Critical Review of the Literature on Signaling Unobservable Product Quality, *Journal of Marketing*, 64(April), 66-79.

Koehn, D. (2003). The Nature of and Conditions for Online Trust, *Journal of Business Ethics*, 3(March), 3-19.

Lewis, D. & Weigert, A. (1985). Trust as a Social Reality, *Social Forces*, 63(4), 967-985.

Luhmann, N. (1979). *Trust and Power*, Wiley: New York.

Luo, X. (2002). Trust Production and Privacy Concerns on the Internet: A Framework Based on Relationship Marketing and Social Exchange Theory, *Industrial Marketing Management*, 31(2), 111-119.

McAllister, D.J. (1995). Affect- and Cognition-Based Trust as Foundations for Interpersonal Cooperation in Organizations, *Academy of Management Journal*, 38(1), 24-59.

McCole, P., Ramsey, E., & Williams, J. (2010). Trust Considerations on Attitudes Towards Online Purchasing: The Moderating Effect of Privacy and Security Concerns. *Journal of Business Research*, 63(9-10), 1018-1024.

McKnight, H.D. & Chervany, N.L. (2002). What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology, *International Journal of Electronic Commerce*, 6(2), 35-59.

Milliman, R.E. & Fugate, D.L. (1988). Using Trust-Transference as a Persuasion Technique: An Empirical Field Investigation, *Journal of Personal Selling and Sales Management*, 8(August), 1-7.

Milne, G.R. & Boza, E. (1999). Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices, *Journal of Interactive Marketing*, 13(1), 5-24.

Mishra, D., Heide, J.B. & Cort, S.G. (1998). Information Asymmetry and Levels of Agency Relationships, *Journal of Marketing Research*, 35, 277-295.

Moorman, C., Zaltman, G., & Deshpandé, R. (1992). Relationships Between Providers and Users of Market Research: The Dynamics of Trust Within and Between Organizations, *Journal of Marketing Research*, 29, 314-328.

Morgan, R. & Hunt, S. (1994). The Commitment-Trust Theory of Relationship Marketing, *Journal of Marketing*, 58, 20-38.

Mutz, D.C. (2005). Social Trust and E-Commerce: Experimental Evidence for the Effects of Social Trust on Individuals' Economic Behavior, *Public Opinion Quarterly*, 69(3), 393-416.

Parasuraman, A. & Zinkhan, G. (2002). Marketing to and Serving Customers through the Internet: An Overview and Research Agenda, *Journal of the Academy of Marketing Science*, 30(4), 286-295.

Rao, A. & Monroe, K. (1996). Causes and Consequences of Price Premiums, *Journal of Business,* 54, 511-536.

Reibstein, D.J. (2002). What Attracts Customers to Online Stores and What Keeps Them Coming Back? *Journal of the Academy of Marketing Science*, 30(Fall), 465-473.

Russell, T. & Lane, W. (2002). *Kleppner's Advertising Procedure*, Upper Saddle River, NJ: Prentice Hall.

Rust, R., Kannan, P.K., & Peng, N. (2002). The Customer Economics of Internet Privacy, *Journal of the Academy of Marketing Science*, 30(4), 455-464.

Schurr, P. & Ozanne, J. (1985). Influences on Exchange Processes: Buyers' Preconceptions of a Seller's Trustworthiness and Bargaining Toughness, *Journal of Consumer Research*, 11(March), 939-953.

Shankar, V., Urban, G., & Sultan, F. (2002). Online Trust: A Stakeholder Perspective, Concepts, Implications, and Future Directions, *Journal of Strategic Information Systems*, 11, 325-344.

Sheehan, K. & Grubbs-Hoy, M. (2000). Dimensions of Privacy Concern Among Online Consumers, *Journal of Public Policy and Marketing*, 19(1), 62-73.

Sipior, J., Ward, B., & Mendoza, R. (2011). Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons, *Journal of Internet Commerce*, 10(1), 1-16.

Strauss, J. & Frost, R. (1999). *Marketing on the Internet*, Prentice Hall: New Jersey.

Sultan, F., Urban, G., Shankar, V., & Bart, I. (2002). Online Trust: A Stakeholder Perspective, Concepts, Implications, and Future Directions, *Journal of Strategic Information Systems*, 11(3-4), 325-344.

Swan, J.E., Bowers, M.R., & Richardson, L.D. (1999). Customer Trust in the Salesperson: An Integrative Review and Meta-Analysis of the Empirical Literature, *Journal of Business Research*, 44(2), 93-107.

Truste.com (2011). *http:www.truste.com*, accessed May, 2011.

Verisign (2011). *http:www.verisign.com*, accessed May, 2011.

Walczuch, R. & Lundgren, H. (2004). Psychological Antecedents of Institution-Based Consume Trust in E-tailing, *Information Management*, 42(1), 159-166.

Williamson, O. (1993). Calculativeness, Trust, and Economic Organization, *Journal of Law and Economics,* 36(April), 487-500.

Yoon, S (2002). The Antecedents and Consequences of Trust in Online Purchase Decisions, *Journal of Interactive Marketing*, 16(2), 47-63.

JOURNAL OF INTERNATIONAL BUSINESS DISCIPLINES

Volume 8, Number 1 May 2013

Published By:
International Academy of Business Disciplines and Frostburg State University

ISSN 1934-1822 WWW.JIBD.ORG