The Effects of Fictitious Customer Testimonials across Different Cultures

Research-in-Progress

Manjul Gupta
Iowa State University
manjulg@iastate.edu

Joey F. George
Iowa State University
jfgeorge@iastate.edu

ABSTRACT
Publishing customer testimonials has become a popular technique to promote online businesses and establish reputation. However, the majority of the research focusing on customer testimonials as a mechanism for boosting a website’s trustworthiness has been conducted within North America. Thus, relatively little is known about how customer testimonials influence perceived deception and trust among web users outside of North America, particularly for non-Western cultures. Even less is known about how web users with different espoused cultural values react and respond to fictitious or misleading customer testimonials. Taking insights from the extant research on deception, trust, customer testimonials, and cross-cultural differences, we develop a conceptual model that posits that there are culture-specific differences in the way web users form their perceived deception and trust when exposed to fictitious customer testimonials.

Keywords
Customer testimonials, Internet scams, Deception, Trust, Cross-cultural differences

INTRODUCTION
Recently, employees of Belkin International, a California-based manufacturer of consumer electronics, were alleged to hire people to write positive testimonials for Belkin products and poor testimonials for the competitors’ products (Chen, 2009; Parsa, 2009). Similarly, Lipovský, Novomeský, Malcho (2011) raised concerns about how antivirus companies (e.g., Registry Cleaner) display false testimonials on their websites to boost credibility of their substandard products. This demonstrates how some companies and online con artists have been exploiting the unique capabilities of Information Technology to target online audiences. Given the sheer number of people who can be targeted through the Internet and the ease with which customer testimonials (CTs) can be controlled and manipulated, publishing fictitious CTs on websites has become a popular confidence trick (Lipovský et al., 2011). Part of the reason for this is the digital environment of the Internet, which offers online con artists absolute freedom to publish fictitious CTs with little fear of getting caught.

Some research in MIS (e.g., Lohse and Spiller, 1998; Quelch and Klein, 1996) suggests that online CTs promote reputation and influence user perceptions of trust. The impact of online CTs has been studied across many disciplines, for example, psychology (Walker, Field, Giles, Armenakis, and Bernerth, 2009), advertising (Appiah, 2006; Wang, 2005), and communications (Hong, 2005; Ott, Choi, and Hancock, 2011). However, the majority of this research has been primarily conducted from a Western perspective and focused on legitimate customer endorsements. Thus, relatively little is known about the impact of CTs outside of North America. Even less is known about how culturally diverse web users react and respond to deceptive “fictitious” CTs. Given the pervasiveness of the Internet and the low cost associated with setting up a con website, there is a real and practical need to study web users from varied cultures and their perceptions of deception when they are exposed to fictitious CTs. Given that con artists can easily customize CTs by accessing the machine's IP address or numerous other sources of information available on the Internet, this need is especially strong in collectivistic cultures (i.e., the cultures who have strong bond with the members of their family, tribe, or nation) who may view CTs originating from their in-groups (i.e., towards whom a person has a sense of respect and loyalty) more positively than the ones originating from the out-group (i.e., towards whom a person feels a sense of competition or opposition) (Tajfel, 1970).
Some past research in MIS has examined how CTs can be manipulated to influence participants’ perceived deception (i.e., the extent to which a user can identify that the information presented on a website is misrepresented, misleading or fabricated) (Maddox, 1982). Grazioli and Wang (2001) randomly assigned participants to buy an item on behalf of their friend from either a real or a forged site. The forged site contained several manipulations (inflated CTs, exaggerated sales, fictitious physical address, etc.). Surprisingly, the manipulations did not result in higher levels of perceived deception, and therefore, a significant percentage of participants were unable to detect deception in the forged site. Participants seemed to rely more on the inflated CTs and other trust building manipulations present on the forged site compared to the real site. In a different experiment, Grazioli and Jarvenpaa (2000) found that exaggerated CTs did not significantly affect participant’s perceived deception. According to them, this could be because individuals are more likely to be swayed by negative information than positive information. Both of these studies (Grazioli and Jarvenpaa, 2000; Grazioli and Wang, 2001) used North American undergraduate students as participants. To the best of our knowledge, the only study that has looked at online CTs outside of North America was conducted by Sia, Lim, Leung, Lee, Huang, and Benbasat (2009). They conducted an experiment to investigate the impact of peer (in-group) CTs on trusting beliefs of Hong Kong and Australian participants by asking them to purchase required course textbooks from an online book store. Peer CTs were found to influence trusting beliefs of Hong Kong as well as Australian participants; however, the impact was more significant for “collectivistic” Hong Kong participants than Australians participants, who are traditionally considered individualistic (i.e., the cultures with loose group ties).

Though these findings are interesting and insightful, the research stated above has a major shortcoming. While the research (e.g., Grazioli and Jarvenpaa, 2000; Grazioli and Wang, 2001) pertaining to manipulated CTs and perceived deception is culturally biased due to the choice of North American participants, the research (e.g., Sia et al., 2009) examining the moderating role of culture on the relationship between CTs and trust has focused solely on legitimate websites featuring genuine CTs. Due to this shortcoming in the extant research, the findings of the former cannot be generalized to non-Western “collectivistic” cultures, whereas the findings of the latter cannot be generalized to situations where deception is present (e.g., scam websites). In other words, the research stated previously fails to shed light on the role of cultural differences that may make web users more or less prone to falling prey to scam websites that feature fictitious CTs. Are web users from some cultures more likely to be deceived by scam websites that display fictitious CTs? Taking insights from the extant research on CTs, culture, deception, and trust, we attempt to answer this research question by developing a conceptual model as shown in Figure 1.

![Figure 1. Conceptual Model](image-url)
LITERATURE AND THEORY

Deception is defined as a “message knowingly transmitted by a sender to foster a false belief or conclusion by the receiver” (Buller and Burgoon, 1996, p. 205). People do get suspicious when they come across deception; however, majority of the times, they are not able to persuade themselves about sender’s deceptiveness due to the inherent “truth bias” (i.e., a presumption that people are honest in general) (Vrij and Baxter, 1999). According to Buller and Burgoon (1996), motivation to deceive and motivation to detect deception play an important role in a deceptive communication. Though there exists an abundance of literature on deception, majority of this research “is based on mundane, low-stakes lies” thereby limiting the generalizability of the findings to the situations that involve more realistic scenarios with high level of risk or significant jeopardy (Burgoon, Hamel, and Qin, 2012, p.324). Depending on whether circumstances pose higher or lower levels of jeopardy, motivation is likely to influence the performance of senders to deceive and receivers to detect deception (Burgoon et al., 2012). Burgoon and Floyd (2000) further contend that motivated deceivers can better control their communication, while motivated receivers are expected to be more suspicious and observant.

The sense of suspicion is perceived deception, which denotes “a belief, held without sufficient evidence or proof to warrant certainty, that a person’s speech or actions may be duplicitous” (Buller and Burgoon, 1996, p. 205). This definition of perceived deception fits well in the context of online deception where a web user does not have enough proof to evaluate the legitimacy of a website and is uncertain whether a website is a scam. According to Buller and Burgoon (1996), if truthful and deceptive judgments are the two opposite extremes of the same spectrum, then perceived deception lies somewhere between the two. A high level of perceived deception is likely to result in judging the sender, which in our case is a scam website, being deceptive. Similarly, when suspicion is low, a web user is likely to believe in the scam website. Since web users’ perceived deception can be reduced by “faking trustworthiness” (Shirky, 2008, p. 26), the process of detecting deception becomes even more complex when a deceptive interaction is taking place over the Internet between a scam website and a web user. Before we go further, let us define the notion of “trust.”

Trust is “a state of perceived vulnerability or risk that is derived from an individual’s uncertainty regarding the motives, intentions, and prospective actions of others on whom they depend” (Kramer, 1999, p. 571). In this paper, we consider a situation where a web user comes across a scam website over the Internet. We assume that the web user has never visited this or a similar scam website before, thus, from his or her point of view there is uncertainty and perceived risk about the motives and intentions of the unknown website (Grazioli and Jarvenpaa, 2000; McKnight, Choudhary, and Kacmar, 2002). In this setting, trust is also contingent on the future actions of the website (Sztompka, 2000). Trust has always been considered a complex construct, and as a consequence, many scholars (e.g., Gefen and Heatl, 2006; McKnight, Cummings, and Chervany, 1998; McKnight et al., 2002) have suggested dichotomizing it into two sub-constructs - trusting beliefs and trusting intentions.

The delineation of trust into trusting beliefs and trusting intentions is based on Fishbein and Ajzen’s (1975) theory of reasoned action (TRA). According to TRA, beliefs and intentions are two distinct constructs. While trusting beliefs reflect whether or not a web user believes that the website is honest and trustworthy, trusting intentions are associated with web user’s willingness to undertake any risks as a consequence of depending on the website (McKnight et al., 1998). Thus, once a web user has formed his or her initial trusting beliefs towards the website, he or she is ready to expose himself or herself to the risk associated with believing in the website (Sia et al., 2009). Drawing upon TRA, McKnight et al. (1998) argue that trusting beliefs lead to trusting intentions. Consistent with this, substantial research (e.g., Lee and Turban, 2001; McKnight et al., 2002) has established trusting beliefs “as important mediators that influence trusting intentions” (Wang and Benbasat, 2007, p.222). Furthermore, given the complexity and confusion surrounding the construct “trust” (Shapiro, 1987a), the recent work in MIS (e.g., Lim, Sia, Lee, and Benbasat, 2006; Sia et al., 2009; Wang and Benbasat, 2007) has primarily focused on web users’ trusting beliefs as the main dependent variable of interest. Since we are more interested in examining how web users evaluate (honesty or trustworthiness) a website after viewing the fictitious CTs, based on the research reviewed in this section, we focus on trusting beliefs rather than trusting intentions.

Customer Testimonials, Perceived Deception, and Trusting Beliefs

Research in marketing and advertising suggests that a typical CT would include a satisfied customer discussing his or her experience about the quality, value, and efficiency of the service provided by the website (O’Guinn, Allen, and Semenik, 2000). Raphel (1997) argues that potential customers are likely to believe in testimonials by routine or everyday customers because, unlike a celebrity or an expert, an average customer is not paid for his or her endorsement. An experiment by Appiah (2006) demonstrated that web users favor websites featuring CTs more than the ones with no testimonials. In the same spirit, Hong (2006) found that the presence of testimonials/quotations was positively associated with the believability of
a healthcare website. Before we go further, we would like to highlight how information technology (IT) has given a new meaning to traditional word-of-mouth (WoM) testimonials.

According to Dellarocas (2003), it is the unique capabilities of IT that have completely transformed traditional WoM into digital WoM. He cites three major differences between the two: (1) online CTs can reach unprecedented level of global audiences at a very low cost, (2) unlike traditional WoM, online CTs can be controlled or modeled, and (3) absence of social-context cues and presence of virtual identities present unique challenges while interpreting online CTs. Thus, unlike traditional WoM, which requires face-to-face interaction thereby making them relatively difficult to manipulate, online CTs can be easily manipulated under the disguise of virtual identities. Furthermore, the low cost associated with the manipulation and easy access to massive Internet audience, makes the use of fictitious CTs well suited for an online con activity.

There is another reason why the use of CTs has been so popular over the Internet, especially by scam websites. Unlike third party seals and news clips, which can be clicked and thereby provide web users the capability to validate if the website is actually registered with the independent agencies (e.g., the Better Business Bureau, TRUSTe), or if the link to a news website actually features a story about the website, CTs are static, and thus cannot be clicked or verified. Another advantage of CTs is the ease with which they can be customized in terms of their origin (e.g., city, state, or an institution) by accessing the IP address of the machine. For example, see what your friends from Buffalo, NY are saying about us or your friends at XYZ University found our services very useful. A tailored CT can create a false belief that the CT originated from the web user’s inner “social group,” resulting in low level of perceived deception, thereby building the “initial trust” in the unknown website (McKnight et al., 2002). A recent field experiment conducted by Jensen, Dinger, Wright, and Thatcher (2013) showed that a customized phishing e-mail reduces the receiver’s perceived deception because the sender seems to identify with the recipient.

However, the significance of these findings may vary because cultural factors can play an important role in how users develop their perceptions of deception and trust over the Internet. Substantial research on deception indicates that there are culturally specific differences pertaining to beliefs about deception (e.g., Mealy, Stephan, and Urrutia 2007). Similarly, research pertaining to online trust indicates that trust is formed differently across cultures. For example, Gefen and Heart (2006) and Greenberg, Wong-On-Wing, and Lui (2008), in their studies comparing online consumers from the United states (U.S.) and Israel, and U.S. and Hong Kong respectively, found cross-cultural differences in the way web users formed their trusting beliefs over the Internet. Therefore, to understand the notion of trust in an online environment, it is important to describe the concept of “culture.”

**Culture**

Culture can be defined as “the collective programming of the mind which distinguishes the members of one human group from another” (Hofstede, 1980, p. 260). To better understand the notion of culture, Hofstede (1980) and Hofstede and Bond (1988) identified five dimensions of national culture: individualism-collectivism, power distance, uncertainty avoidance, masculinity-femininity, and long-term orientation. Though each of these five cultural dimensions captures some unique aspect of the multi-faceted “culture” construct, prior cross-cultural research has established individualism-collectivism (IND) (i.e., extent to which individuals are integrated into groups) as the most prominent dimension for capturing cross-cultural differences (Hofstede, 1980; Triandis, 2001). Moreover, compared to other cultural dimensions, only IND is capable of assessing the degree to which individuals differentiate between in-groups and out-groups.

Tajfel (1970) argues that in-groups and out-groups can be classified into “we” versus “they,” such that a person has a sense of respect and loyalty towards the “we” or in-group and a sense of competition or opposition towards the “they” or out-group. A family, tribe, village, religious community, nation, and work group are all examples of in-groups with which an individual can identify (Triandis, 1996), while out-groups may consist of people (e.g., complete strangers, foreigners) with whom an individual does not relate. Since we are primarily interested in studying whether fictitious CTs invoke a false belief of “unit grouping” in the same way among culturally varied web users and given no other cultural dimension captures the extent of individuals’ display of in-group favoritism and out-group prejudice (Sia et al., 2009), we focus on IND in this paper.

While Hofstede (1980) defined culture at a macro “national” level, research in cultural psychology and psychological anthropology consider culture a dimension of an individual’s personality (Srite and Karahanna, 2006). Consistent with this, Srite and Karahanna (2006) contend that individuals differ in the degree to which they espouse national cultural values, and thus these values should be examined at an individual level. Thus, in this paper, we treat IND as the extent to which a web user values his or her in-group as opposed to the out-group.
HYPOTHESES

While in-groups and out-groups exist within both individualistic and collectivistic cultures (Gomez, Kirkman, and Shapiro 2000), people in collectivistic cultures are affiliated with a selected few in-groups, compared with individualistic cultures in which people belong to many in-groups. Because people in individualistic societies tend to act based on their own self beliefs rather than the norms of their in-groups (Triandis 2001), collectivistic cultures value “group-orientation,” while individualistic cultures value “self-orientation” (Hofstede 1980). Individualistic societies are universalistic in nature and tend to favor both their in-groups and out-groups equally. On the other hand, collectivistic societies are generally considered particularistic and tend to discriminate against out-groups and favor in-groups (Gomez et al., 2000). Hui, Triandis, and Yee (1991) have also demonstrated that people in collectivistic cultures reward their in-group members more than the members of the out-group. Sumner (1906) explains the behaviors towards in-groups and out-groups in an excellent manner:

The relation of comradeship and peace in the we-group and that of hostility and war towards others-groups are correlative to each other. The exigencies of war with outsiders are what make peace inside, lest internal discord should weaken the we-group for war. Sentiments are produced to correspond. Loyalty to the in-group, sacrifice for it, hatred and contempt for outsiders, brotherhood within, warlikeness without—all group together, common products of the same situation. (p. 12–13)

Thus, we expect that web users with espoused collectivistic values are more likely to be deceived by fictitious CTs that feature someone from their inner group compared to the one provided by a foreigner or someone from their out-group. Therefore:

Hypothesis 1: The origin (in-group or out-group) of fictitious customer testimonials will negatively affect web users’ perceived deception of the website such that users with espoused collectivistic values are more likely to be deceived by fictitious in-group customer testimonials than fictitious out-group customer testimonials.

Since the traditional indicators of deception (e.g., facial expressions, tone of voice, and irregular postures), which people in general rely on to detect deceptive behavior, do not seem to work over the digital environment of the Internet, a CT from a perceived similar rather than from a complete stranger or foreigner is likely to influence web users’ trusting beliefs in a scam website. However, as suggested by cross-cultural research discussed previously, we expect that this influence on web users’ trusting beliefs in a website will be more for web users with espoused collectivistic values than individualistic values. Based on this, we hypothesize:

Hypothesis 2: Fictitious in-group customer testimonials will have a stronger influence on collectivistic web users’ trusting beliefs in the website compared to web users with espoused individualistic values.

Our conceptual model (see Figure 1.) also proposes a relationship between perceived deception and trusting beliefs. Buller and Burgoon (1996) suggest that perceived deception refers to uncertainty pertaining to judging the sender either completely honest or completely dishonest. Thus, if a web user considers a scam website trustworthy, he or she is likely to have a low level of perceived deception and vice versa. In other words, perceived deception negatively influences trusting beliefs. Consistent with this, the research linking perceived deception and trust (Grazioli and Jarvenpaa, 2000; Grazioli and Wang, 2001) has found significant negative effects of perceived deception on trust. Therefore, taking insights from Buller and Burgoon (1996) and the work of Grazioli and colleagues, we propose:

Hypothesis 3: The greater the web user’s perceived deception towards the website, the lower the web user’s trusting beliefs associated with that website.

METHODOLOGY

For this study, we will conduct a controlled laboratory experiment. Subjects will be graduate level students, who will be recruited from a large university in the U.S. and in China. The primary reason for selecting subjects form these two countries is the significant difference between their individualism (IDV) indices, which is 15 for China and 91 for the U.S. (Hofstede, 1980). The experimental task will involve subjects browsing a website of a non-chain restaurant. Half of the subjects will access the real website, while the remaining half will access the forged website. The real site will display genuine CTs, while the forged site will contain fictitious CTs. CTs will be varied by having a website version either with in-group (e.g., someone from subjects’ own country or local region) CTs or out-group (e.g., someone outside of subjects’ country or local region) CTs. After browsing through the website, subjects will be asked to complete a questionnaire containing measures of perceived deception and trusting beliefs. The measures of perceived deception will be adapted from Grazioli and Jarvenpaa (2000) and the scale items to measure trusting beliefs will be derived from Sia et al. (2009). Following this, subjects’ espoused individualistic-collectivistic values will be assessed using the scale developed by Srite and Karahanna (2006). Once data are collected, we plan to test the previously stated hypothesis using structural equation modeling (SEM). For this study, we will control for all the variables that may potentially impact subjects’ trusting beliefs or perceived deception. Therefore,
consistent with previous research, we will control for subjects’ age and gender and their experience with the Internet (Sia et al., 2009).

CONCLUSION
The primary insight that guides this paper is that web users with espoused collectivistic values, due to their in-group favoritism and out-group hostility, are more likely to be deceived by fictitious CTs when the person endorsing the website appears to be a member of the same in-group as the web user. Recently, Xiao and Benbasat (2011) raised concerns about the possible exploitation of online CTs in collectivistic cultures. Given the vast majority of people in this world live in collectivistic societies, the investigation of the research question stated in this paper is of practical significance. Furthermore, according to Internet World Stats (2012), 44.8% of all Internet users are from “collectivistic” Asia and as global Internet usage increases, this number is likely to rise as well thereby making the insights provided in this conceptual paper important for law enforcement agencies like the Internet Crime Complaint Center, whose mission is to protect online users from con artists.

Our model predicts that web users with espoused individualistic values, due to their propensity to favor both in-groups and out-groups without any bias, are less likely to discriminate between in-group and out-group CTs, making them less prone to getting deceived by fictitious CTs as opposed to web users with espoused collectivistic values.

Our approach is unique because we view Internet deception and trust from a non-Western perspective. By doing this, we have taken a small step to address the concerns of “parochialism” in the field of information systems research (Galliers and Meadows, 2003).

Since this is a conceptual paper, the proposed hypotheses need to be empirically tested before any conclusions can be made. Furthermore, we have used Hofstede’s cultural perspective in this paper; however, a cross-cultural framework more recent than Hofstede’s called “the GLOBE study” (Javidan, Dorfman, Sully de Luque, and House, 2006) has been gaining significant attention from cross-cultural researchers.

REFERENCES


