Available online at www.sciencedirect.com
ScienceDirect
Journal of Interactive Marketing 25 (2011) 145–158
JOURNAL OF INTERACTIVE MARKETING
www.elsevier.com/locate/intmar

Third-party Privacy Certification as an Online Advertising Strategy: An Investigation of the Factors Affecting the Relationship between Third-party Certification and Initial Trust

Kyongseok Kim * & Jooyoung Kim

Department of Advertising & Public Relations, Grady College of Journalism & Mass Communication, University of Georgia, Journalism Bldg, Athens, GA 30602-3018, USA

Available online 13 November 2010

Abstract

The purpose of this study is to assess the possibility of implementing an online advertising strategy using a well-known third-party privacy seal located on the order page of an unfamiliar online retailer. An online experiment was conducted with 223 participants using a 2 (third-party seal: present vs. absent)×2 (purchase-decision involvement: low vs. high)×2 (disposition to trust: low vs. high)×2 (privacy-protection self-efficacy: low vs. high) between-subjects design. The results provide evidence of trust transference from a well-known third-party seal to an unfamiliar retailer website, indicating that seal presence raised initial trust in the website and that the effects of seal presence were mediated by perceived privacy empowerment. Results also indicate that the seal effects were moderated by the level of purchase-decision involvement, disposition to trust, and self-efficacy. Theoretical explanations and managerial implications are discussed.

Keywords: Third-party privacy certification; Initial trust; Perceived privacy empowerment; Purchase-decision involvement; Disposition to trust; Self-efficacy

Introduction

The scale of e-commerce has grown substantially over the past decade as an alternative to brick-and-mortar stores (Fox 2008). E-commerce is convenient and time saving, but several consumer concerns have emerged with its rapid large-scale growth (Odom, Kumar, and Saunders 2002). Among these concerns, privacy has been consistently identified as the most pressing (Rifon, LaRose, and Choi 2005).

To survive the highly competitive Internet marketplace, online retailers have constantly relied on customers' personal information to tailor products and services to their specific needs. However, as this information has been frequently abused by some of these online retailers, concerns about privacy have also increased (Nam et al. 2006). Specific privacy risks that Internet users face range from inadvertent disclosure of personal information, to unwanted contact (e.g., spam mail), to use of personal data by third parties, to hacking and identity theft (McCole, Ramsey, and Williams 2010). In fact, online consumers are known to be most concerned about privacy and safety, contradicting the common assumption that cost and convenience are their predominant concerns (Jiang, Jones, and Javie 2008). In light of this discovery, traditional marketing promotion efforts might not always be successful when applied to e-commerce.

Third-party privacy certification has evolved as a major self-regulatory practice to address consumers' concerns about privacy during online transactions. Prior studies have investigated the effects of third-party certification on promoting initial trust in unfamiliar websites (e.g., Chang and Cheung 2005; Wang, Beatty, and Foxx 2004), considering that most small-scale and unknown online retailers rarely establish ongoing relationships with consumers. In other words, examining methods for building initial trust, which happens at the early stage of the consumer–retailer relationship and does not require extensive interaction, can help illuminate an important problem in e-commerce.

* Corresponding author.
E-mail addresses: kimks81@uga.edu (K. Kim), jykim@uga.edu (J. Kim).

1094-9968/$ - see front matter © 2010 Direct Marketing Educational Foundation, Inc. Published by Elsevier Inc. All rights reserved.
doi:10.1016/j.intmar.2010.09.003

Drop-off rates at the point of purchase at online stores (more than 30%) are known to be significantly higher than they are at offline stores (less than 3%) (Li and Chatterjee 2005). This fact derives from online consumers' concerns about privacy, for they must provide online retailers with their personal and payment information to complete purchases. However, no study has examined the effects of posting a third-party seal in a particular location on a retail website. Accordingly, the current study proposes that posting a third-party seal on the order page of an unfamiliar website would encourage both initial trust in the website and intent to purchase by alleviating privacy concerns.

The absence of a theoretical explanation for the cognitive process that mediates the effects of third-party certification constitutes a major limitation of previous studies. For this reason, this study uses the construct *perceived privacy empowerment* (PE)—a psychological construct related to "the individual's perception of the extent to which they can control the distribution and use of their personally identifiable information" (van Dyke, Midha, and Nemati 2007, p. 73)—as an antecedent of initial trust and explores its mediating role in the way a seal might affect initial trust. Moreover, given that few studies have paid attention to moderating factors that could affect the relationship between third-party certification and initial trust, this study examines the influences of three individual characteristic variables, *purchase-decision involvement* (PDI), *disposition to trust* (DT), and *privacy-protection self-efficacy* (PSE), upon the effects of third-party certification.

Theoretical Framework and Hypotheses

Internet Privacy, Privacy Concerns, and Privacy Assurances

The commercial development of the World Wide Web has engendered a trust gap between online consumers and retailers, a gap that has centered on the privacy of personally identifiable information (Moores and Dhillon 2003). Because there is little consensus in e-commerce literature on what Internet privacy means (Dinev and Hart 2005), a more practical way to introduce the concept is through its relationship with security, a term with which privacy is easily confused (Belanger, Hiller, and Smith 2002). In fact, these two concepts are simultaneously interrelated and distinct. Privacy requires security, given that privacy cannot be protected without technologically secure methods for storing and transmitting personal information. However, apart from secure storage and transmission of personally identifiable information, online consumers might also worry that their personal information will be collected and sold to third parties without their knowledge or consent (Chellappa and Sin 2005; Hoffman, Novak, and Peralta 1999). Accordingly, security and privacy are often regarded as "hard" and "soft" trust components, respectively (Head and Hassanein 2002). In particular, hard trust centers on technological solutions for providing safe exchanges of information, whereas soft trust encompasses such concerns as product quality and privacy, which cannot be managed by technology alone. For this reason, Internet privacy is often addressed not only by information systems researchers but also by marketing communication researchers.

In the e-commerce literature, concerns about privacy have been declared a major obstacle to consumer engagement in online transactions (e.g., Miyazaki and Krishnamurthy 2002; Rifon, LaRose, and Choi 2005; van Dyke, Midha, and Nemati 2007). One method for alleviating consumers' privacy risks is to provide them with privacy assurances (Mauldin and Arunachalam 2002). To this end, the U.S. e-commerce industry has set up self-regulatory practices that focus on the use of privacy policy statements and third-party privacy certification seals (Culnan 2000; Moores and Dhillon 2003).

A privacy policy statement is the comprehensive description of a website's information practices, and most commercial websites have one (Milne and Culnan 2004). Nevertheless, the effectiveness of privacy policy statements in reducing consumers' concerns about privacy is still debatable. First of all, privacy policy statements are often too long to be useful because Internet users may not be motivated to spend their time and effort reading the fine print (Head and Hassanein 2002). In addition, these statements often include numerous technical terms that make them difficult for average users to comprehend (Belanger, Hiller, and Smith 2002).

The other privacy assurance, constituting the focus of this study, is the third-party privacy certification seal. To obtain a seal from a third-party authority, the online business is required to undergo a rigorous review process that assesses its information practices according to the set of standards built upon Fair Information Practices (FIPs) (Benassi 1999; Federal Trade Commission 1998). The costs of using third-party seals vary with the revenues generated by online businesses; the greater the revenue, the higher the costs of initial approval and continual monitoring (Miyazaki and Krishnamurthy 2002; Moores and Dhillon 2003). Accordingly, for small-scale online retailers, third-party certification offers a low-cost, easily-adoptable method for building consumer trust.

Third-party seals do offer some practical advantages over privacy policy statements. First, third-party seals symbolically represent third-party authorities, an immediately visible way to reassure consumers that the online business respects consumer privacy (Liu et al. 2005). Moreover, the effectiveness of privacy policy statements is difficult to assess consistently because they differ from website to website and are subject to change at the discretion of the business (Anton and Earp 2004). In contrast, third-party seals measure privacy effectiveness more consistently because they confirm that a website's information practices are in line with FIP standards (Lwin and Williams 2003).

Hypotheses

A total of eight hypotheses were developed. First, a series of relationships between two initial trust constructs, *trusting beliefs* (TB) and *trusting intentions* (TI), and *perceived privacy empowerment* (PE) was examined to ensure that perceived privacy empowerment is a significant mediator of initial trust (H1 and H2). Once these hypothesized relationships were validated, the main effects of third-party certification on perceived privacy empowerment, trusting beliefs, and trusting intentions were tested to explain how third-party certification