ARTICLE IN PRESS

Journal of Retailing and Consumer Services ∎ (∎∎∎∎) ∎∎∎–∎∎∎

Contents lists available at ScienceDirect

Journal of Retailing and Consumer Services

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

Privacy versus reward: Do loyalty programs increase consumers' willingness to share personal information with third-party advertisers and data brokers?

Tun-Min (Catherine) Jai [a,*], Nancy J. King [b]

[a] College of Human Sciences, Texas Tech University, Human Sciences 601, 1301 Akron Avenue, Lubbock, TX 79409, United States
[b] College of Business, Oregon State University, Bexell Hall 336, Corvallis, OR 97331, United States

ARTICLE INFO

Keywords:
Consumer loyalty
Commitment
Consumer data
Information privacy
Privacy segment index
Data brokers

ABSTRACT

This research reports that U.S. online shoppers significantly identify third-party advertisers and data brokers as separate agents and display different attitudes toward sharing their PI in the context of online retailing. Applying Westins' Privacy Segmentation Index, the results showed that enrollment in multiple loyalty programs significantly predicts Privacy Pragmatic shoppers' willingness to share personal information, while consumer commitment significantly increases both the Privacy Unconcerned and Pragmatist groups' willingness to share. Conversely, this is not the case for Privacy Fundamentalists. Age and gender also played important roles in predicting consumers' willingness to share their PI with advertisers and data brokers.

Published by Elsevier Ltd.

1. Introduction

Consumer data has never been more important than it is today in the retailing industry. Using data mining technology, marketers can easily extract a vast amount of U.S. consumers' personal data with only their names and an email addresses. These data may include online/offline shopping history, social media preferences, and information about any loyalty programs the consumer is a member of, accompanied by the consumers' demographic information (Stein, 2011). For many U.S. citizens, it is common experience to be recognized immediately by a particular website when visiting the website a second time. Consumers may even be presented with re-targeted banner ads after they leave a website. Although these behavioral-targeted services often seem harmless to consumers, what this seemingly endless marketing activity suggests is that the collected consumers' data have been sold or shared for secondary marketing purposes. Market research has shown that U.S. consumers believe the internet is not well-regulated (TRUSTe, 2012), and it appears that consumers' largest privacy concerns are the result of third-party sharing and use of their information for secondary purposes.

On the other hand, having access to accurate customer data is essential to operate an effective customer relationship management (CRM) program (Abbott et al., 2001). Thus, the collection of consumer data is an almost universal practice of commercial websites, although the methods of collection, as well as the scope and manner of use of collected information, varies from business to business (Hoy and Phelps, 2009; Langenderfer and Miyazaki, 2009; Schwaig et al., 2006). Consumer information privacy has been defined as "the consumer's ability to control (a) the presence of other people in the environment during a market transaction or consumption behavior and (b) the dissemination of information related to or provided during such transactions or behaviors to those who were not present" (Goodwin, 1991, p. 152). By applying Social Contract Theory, researchers found consumers performed a benefit-cost evaluation (or "trade-off") when they engaged in online information exchange (Culnan and Bies, 2003; Malhotra et al., 2004; Park et al., 2012). This trade-off has been studied offline as "privacy calculus," which measures the usage of personal information (PI) against the potential negative consequences of disseminating personal information (Laufer and Wolfe, 1977; Milne and Gordon, 1993). In the context of online privacy, consumer's willingness to share their personal information online involves evaluating the benefits and risks of releasing personal information (Awad and Krishnan, 2006; Jai et al., 2013).

In the realm of internet technology, many consumers have experienced an overwhelming amount of spam email, unsolicited marketing activity, and financial fraud. These undesirable circumstances may be perceived as the cost of disseminating personal information. On the other hand, previous research has shown that consumers may be willing to disclose their personal

* Corresponding author. Fax: +1 806 742 3042.
E-mail address: catherine.jai@ttu.edu (T.-M. Jai).

http://dx.doi.org/10.1016/j.jretconser.2015.01.005
0969-6989/Published by Elsevier Ltd.

information to obtain "free" information, personalized content (Pastore, 1999), prizes, loyalty program memberships (Earp and Baumer, 2003), discounts (White, 2004), or some other form of "fair" exchange (Culnan and Bies, 2003). Researchers have suggested that by segmenting consumers by privacy concerns, online marketers are better able to target these consumers without violating consumer privacy expectations (Dolnicar and Jordaan, 2007). Although previous studies have made significant progress towards understanding how consumers' general privacy concerns influence their online disclosures of information, there is a lack of an empirical study that investigates customers' willingness to give online retailers permission to disclose their personal information to other marketers for secondary marketing purposes. In particular, our research questions are:

(1) How likely are consumers to be willing to share their personal data with third-party advertisers and data brokers when they shop online, and does the consumer's willingness to share his or her personal information vary between third-party advertisers and data brokers?
(2) What are the effects of age, gender, and consumer loyalty (commitment and amount of loyalty program enrollments) on consumers' willingness to give online retailers permission to share personal information with third-party advertiser and data brokers?
(3) Do the effects of age, gender, and consumer loyalty on the willingness to share personal information apply to different consumer privacy segments?

2. Literature review and hypotheses development

2.1. Sharing PI with third-party advertisers and data Brokers

The importance of customer relationship management (CRM) is increasingly being recognized (Kumar and Reinartz, 2012). Customer relationship management utilizes information-intensive strategies that help retailers to serve shoppers better at all contact points (Sin et al., 2005). Many personalized marketing practices, such as behavioral targeting advertisement, would be impossible without appropriate consumer data. Practices such as these utilize consumer data to build firm-customer relationships by leveraging rigorous linking technology to targeted marketing activities (Harding et al., 2004). As a result, consumers' personal information (PI) (e.g. name, geographic location, income, family size, brand preference, and browsing history) becomes a critical asset for both online retailers and third-party advertisers. In their study of young consumers' perceptions of unsolicited behavioral tracking for personalized advertisements, have found that the online shoppers were concerned about online retailers disseminating their personal information with outside companies for secondary marketing purposes.

Another practice that online retailers may also be involved in is Data Enhancement. This practice occurs when a company appends data obtained from third-party sources, such as data brokers, to information it collects directly from consumers. U.S. consumers currently do not have a choice to prevent companies from enhancing their data as the practice is not regulated. Many consumers consider data enhancement to be out-of-context data sharing, and they specifically object to allowing companies to enhance their data without providing them with a choice (FTC, 2012). There is a fine line between providing personalized services and violating an individual's privacy. The FTC (2012) report suggests "…the practice of enhancing online cookie data or IP addresses with offline identity data ….should be subject to consumer choice" (p.43). Thus, this empirical study is warranted to identify who is more likely to give retailers permission to share personal information with third-party advertisers and data brokers and by what means consumers are motivated to give retailers permission for data sharing. Accordingly, the following hypothesis was developed:

H1. There are significant differences between consumers' willingness to give online retailers permission to share their personal information with third-party advertisers and data brokers.

2.2. Privacy segment index

Privacy is a complicated concept and the degree of privacy concerns may vary from individual to individual (Larose and Rifon, 2007; Milne and Rohm, 2000). Studies have found that, in general, concern about privacy has a negative impact on online consumers' intention to disclose their personal information (Li et al., 2011). Both government agencies and researchers have been called to examine privacy decision-making while taking into account situation-specific factors (FTC, 2009; Malhotra et al., 2004; Li et al., 2010). In order to better understand the relationship between consumers' privacy preferences and their privacy related behaviors, from 1978 to 2004, Dr. Alan Westin created Privacy Segmentation Indexes (PSI) to classify consumers according to their privacy concerns into three groups: privacy fundamentalists, privacy pragmatists and privacy unconcerned groups. Westin's classification is based on a consumer's agreement with three statements: "(1) consumers have lost all control over how personal information is collected and used by companies; (2) most businesses handle the personal information they collect about consumers in a proper and confidential way; and (3) existing laws and organizational practices provide a reasonable level of protection for consumer privacy today" (Kumaraguru and Cranor, 2005, p. 13). The Privacy Fundamentalists group (about 25% of the national public) was defined as "*This group sees privacy as an especially high value.… [they] think more individuals should simply refuse to give out information they are asked for*" (Harris Interactive, 2002, p. 20). The Privacy Pragmatists group (about 55% of the national public) was defined as "*This group weighs the value to them and society of various business or government programs calling for personal information, examines the relevance and social propriety of the information sought, wants to know the potential risks to the privacy or security of their information, looks to see whether fair information practices are being widely enough observed, and then decides whether they will agree or disagree with specific information activities—with their trust in the particular industry or company involved being a critical decisional factor*" (Harris Interactive, 2002, p. 20–21). The Privacy Unconcerned group (about 20% of the national public) was defined as "*This group…… supports the benefits of most organizational programs over warnings about privacy abuse, has little problem with supplying their personal information to government authorities or businesses*" (Harris Interactive, 2002, p. 21). In the present study, we followed Westin's Privacy Segmentation Index stated in the Harris interactive (2002) study to classify our respondents. The respondents who agreed (strongly or somewhat) with the first statement and disagreed (strongly or somewhat) with the second and third statements were classified as Privacy Fundamentalists. The respondents who disagreed (strongly or somewhat) with the first statement and agreed (strongly or somewhat) with the second and third statements were classified as the Privacy Unconcerned group. The respondents who were not included in the unconcerned or fundamentalist groups were classified as the Privacy Pragmatists group.

Many who research privacy have used these privacy indexes as benchmarks with which to compare their own survey results