9-2009

Privacy Concern and Online Personalization: The Moderating Effects of Information Control and Compensation

David G. Taylor
Sacred Heart University, taylord44@sacredheart.edu

Donna F. Davis
Texas Tech University

Ravi Jillapalli
Texas Tech University

Privacy concern and online personalization: The moderating effects of information control and compensation

September 2008

David G. Taylor*
University of North Texas

Donna F. Davis
Texas Tech University

Ravi Jillapalli
Texas Tech University

*** Primary contact information:**
Department of Marketing & Logistics
College of Business Administration
University of North Texas
Denton, Texas 76201
Phone: (940) 565-3174
Email: davidtaylor@unt.edu

Privacy concern and online personalization:
The moderating effects of information control and compensation

Abstract

Firms have at their disposal an increasing amount of personal information about consumers gathered through various means. Studies find that personalizing online interactions improves customer relationships and increases desirable behaviors, such as positive word-of-mouth and increased purchase intent. However, other research suggests that the use of personal information stimulates privacy concern, which has a negative effect on behavior. This study examines potential moderators of the negative effects of privacy concern on behavioral intentions in the context of personalized online interactions. Results show that increasing perceived information control reduces the negative effect of privacy concern on behavioral intentions. In contrast, the offer of compensation has no effect on the relationship between privacy concern and behavioral intentions. However, compensation increases the salience of trust to privacy concern.

Keywords: privacy concern, personalization, compensation, non-self-disclosed information, online trust

Privacy concern and online personalization:
The effects of the use of non-self-disclosed information

1. Introduction

Advances in technology that enable personalization have outpaced marketers' understanding of the implications of personalizing online interactions. Today's sophisticated monitoring systems, robust databases and data mining tools allow companies to unobtrusively gather information about individual transactions and use that information to personalize interactions [28, 38]. For example, demographic information can be obtained relatively easily from customers through site registrations, warranty forms and other methods of self-disclosure. Web site technology allows organizations to also gather non-self-disclosed information via clickstream data that can be used to profile and target individual consumers with cookies and tracking software [36]. In addition to internal transaction data, companies can purchase and link external information collected through scanner data, loyalty programs and store credit cards [18]. As technology improves, the ability to effectively personalize interactions is quickly becoming an important factor in the competition for online consumers.

The concept of interactive marketing advocates personalization in order to create an electronic dialogue with customers [6]. Internet-based interactive marketing presents perhaps the best opportunity to not only collect, but also to utilize transactional, behavioral and demographic data to personalize online interactions. Online personalization is defined as matching categorized content to profiled users, in effect filtering content based on a company's determination of the content's relevance to the user [5]. Previous academic and industry research supports the notion that online personalization has a positive effect on customer response. For example, personalized e-mail messages have been found to generate higher click-

through rates compared to generic messages [44]. Similarly, using personal information to target consumers has been shown to improve response rates for online advertising [33]. These studies tend to lend credence to the practice of personalization as a means to engage consumers in online interactions.

However, other research suggests a strong positive relationship between personalization and privacy concerns [43]. It is widely reported that consumers are becoming more concerned about threats to privacy in the online environment. Industry studies find up to 80 percent of Americans are very or somewhat concerned about the issue [18]. It is not surprising, then, that research shows a negative relationship between privacy concern and purchase behavior [3, 13, 43]. This tension between personalization and privacy concern raises an important question: How can marketers balance the firm's desire to personalize online interactions with consumers' privacy concerns in ways that improve consumers' engagement and response?

The marketing literature suggests several concepts as useful in understanding how to attenuate the negative effect of privacy concern on behavioral intentions in the context of online interactions. These concepts can be broadly classified as consumer attitudes, such as online trust, and situational variables, such as the degree of information control and compensation offers afforded by a particular Web site [3]. These concepts are variously proposed to have direct, mediating and moderating effects on privacy concern and behavior. In this study, we examine the role of generalized online trust, information control and compensation on the relationship between privacy concern and behavioral intentions.

The purpose of this research is to explore the effects of privacy concern on behavioral intentions in the context of online personalization. To accomplish our objective, we developed an online travel site with the capability to deliver personalized messages using both self-

disclosed and non-self-disclosed information. Using this tool, we tested a basic conceptual framework in which generalized online trust reduces privacy concern and privacy concern reduces behavioral intentions. We then examined the moderating effects of perceived information control and compensation offers (see Figure 1).

We begin with a discussion of the conceptual framework and develop our hypotheses. Next, we describe the research method and present the results of hypothesis testing. We then discuss our findings and conclude with theoretical and practical implications.

<Figure 1 about here>

2. Conceptual framework and hypotheses

2.1 Personalization and privacy concern

Personalization requires collecting and using information about an individual consumer to tailor content targeted to the individual. This information may be voluntarily self-disclosed by a consumer or non-self-disclosed, that is, collected without the consumer's full knowledge and consent. Consumers frequently self-disclose information online in order to gain access to information or to complete transactions. Self-disclosure can be distilled to the concept of providing others with personal information about oneself [24]. Research shows that consumers are less concerned about privacy when marketers request permission to collect and use information to tailor communications [41].

However consumers often are not aware that personal information is being collected until they receive some form of personalized communication from the firm [47]. We define such information as non-self-disclosed information: personal information that is collected by another party without the full knowledge and consent of the individual consumer. Some privacy

literature refers to unvolunteered data that is collected through transactional and purchase data, as well as monitored Web activity [34]. We expand this concept to include not only unvolunteered information collected during transactions, but also information collected by or merged with other information sources, such as purchase data gathered in loyalty card programs. This type of data is inherently different from self-disclosed data because consumers are often unaware that this information is being compiled and have no control over the collection, storage and use of such information [46]. Although much of the data collected surreptitiously could be perceived by consumers as a privacy violation, it is likely that they are not aware of online tools, such as cookie deposits, used to collect personal data [36].

A significant stream of research aims to explain the antecedents and outcomes of online privacy concern. Phelps et al. [43] suggest that privacy concern consists of consumers' perceptions regarding exchange relationships with marketers that gather and use personal information and the resulting behaviors. Modern legal interpretations of the concept of privacy center around four dimensions [45]: 1) intrusion into private affairs; 2) public disclosure of private facts; 3) publicity which places the person in a false light and; 4) appropriation or using the person's image or identity for someone else's advantage. Westin (1967) defines privacy as the claim of individuals to determine for themselves when, how and to what extent information about them is communicated to others. Goodwin [17] narrows the definition of informational consumer privacy to consider the specific content of information that is stored in a database and the likelihood that this data will actually be used to harm the individual. However, the essence of privacy is essentially unchanged from more than a century ago, when Warren and Brandeis [56] defined it as the right to be left alone.

In the online purchasing context, this right to be left alone primarily relates to information. Privacy can be interpreted as the ability to control the disclosure and use of personal information, and doing business with a Web site "typically necessitates the divulgence of large amounts of personal information which is either necessary for the transaction (for example, credit card information, delivery details) or is desired by the e-business" [51, p. 101]. Thus a tension is created between the consumer's need to divulge information for completion of the transaction and his or her desire to maintain control over personal information. The result can be a level of discomfort in the form of privacy concern.

Academic studies often conceptualize privacy concern as a second-order construct [3, 51]. For example, Milne [36] conceptualizes consumer privacy as a second-order construct with two dimensions: consumer knowledge and control. He suggests that consumer privacy concerns are lowest when a consumer's knowledge of information being collected and used is high, and the consumer's control level is also high. Similarly, Sheehan and Hoy [48] also view privacy concern as a second-order construct and identify five dimensions of online privacy concern: 1) awareness of information collection; 2) usage of information; 3) information sensitivity; 4) familiarity with the entity and; 5) compensation. Their findings support the notion that privacy concern decreases as information control (comprised of awareness of collection and usage of information) increases.

Drawing from Dinev and Hart [9], the present study operationalizes privacy concern as a single-dimension construct relating to concerns about the loss of privacy from information disclosure and collection. We adopt the definition that is most frequently used in the marketing literature: Privacy concern is the customer's concern for controlling the acquisition and subsequent use of information that is generated or acquired in online transactions [3].

2.2 Trust and privacy concern

In the marketing literature, trust is generally viewed as an attitude or belief. For example, Moorman et al. [39] define trust as the willingness to rely on an exchange partner in whom one has confidence. Morgan and Hunt [40] define trust as confidence in an exchange partner's reliability and integrity. These definitions focus on the beliefs and behaviors of the party who trusts. Other research extends the concept to include attributes of the target of trust. For example, Doney and Cannon [11] define trust as the perceived credibility (ability to keep promises) and benevolence (interest to seek joint gain) of a target of trust. Garbarino and Johnson [16] integrate the psychological state of an individual who trusts with attributes of the target of trust in their study of trust between consumers and an organization. They define trust as customer confidence in the quality and reliability of the services offered. Using a similar definition of trust, Gwinner, Gremler and Bitner [20] find the psychological benefits of confidence and trust to be more important than special treatment in strengthening consumer relationships with firms.

In an online context, trust takes on added importance. The lack of faith between consumers and most businesses on the Web is viewed as a major barrier to online commerce [22]. The nature of online trust has been conceptualized in different ways. For example, Luo [31] draws from the work of Zucker [58] to propose three mechanisms for online trust production: character-based trust (based on defining characteristics), process-based trust (based on past exchanges or future expectations) and institution-based trust (tied to formal societal structures). Liu et al. [29] suggest that trust may be internalized as a personality trait based on previous experiences [2] or a belief that one party respects the intentions, actions and integrity of

another party during an online transaction [25]. Consistent with these studies and Doney and Cannon [11], the present study operationalizes trust as a generalized belief in the benevolence and competency of online firms with regard to the usage and safeguarding of personal information.

Both trust and privacy concern have been identified as the most relevant antecedents to online behavior [22]. Numerous studies provide evidence for a negative correlation between trust and privacy concern in online transactions [e.g. 10, 54], but the direction of the relationship is unclear. Chellappa and Sin [4] found correlations but no direction, while Culnan and Armstrong's [7] model implies trust as an antecedent of the "privacy leverage point" at which consumers weigh benefits and risks of the transaction. Other studies, however, model privacy concern as an antecedent of trust [e.g. 3, 30, 53]. The discrepancies around the direction of causality between trust and privacy concern may be an issue of generalization; generalized trust reduces situational privacy concern when the consumer receives a signal such as personalized information, while generalized privacy concern reduces trust in a specific company. Based on previous research, we expect that generalized online trust will reduce the level of privacy concern when information about a consumer is used to personalize an offer on a Web site.

H1: The level of generalized online trust is negatively related to the level of privacy concern.

2.3 Privacy concern and behavioral intentions

The construct of behavioral intentions is drawn from the work of Fishbein and Ajzen [14] and the theory of reasoned action, in which intention is defined as the decision to act in a particular manner. In subsequent research, intentions are operationalized as the likelihood that one will perform a behavior [27] or as an estimate of performing a behavior in the future [49].

Behavioral intentions are conceptualized as the likelihood that a consumer will engage in desired behavior, including making future purchases, spreading positive word-of-mouth or expressing favorable opinions.

The perceived risk of losing one's privacy itself – as opposed to the risk of actual economic loss resulting from the loss of private data – is enough to negatively impact behavioral intentions [10]. Van Slyke et al. [54] were unable to find a negative effect of privacy concern on consumers' willingness to transact with a Web merchant. However, the research of Castañeda and Montoro [3] suggests a strong negative correlation between privacy concern about the collection of data and trust, which is positively correlated with purchasing intentions. Thus, we expect privacy concern will have a negative influence on behavioral intentions.

H2: The level of privacy concern is negatively related to behavioral intentions.

2.4 Moderating effects of information control

Empirical studies suggest that control of information is critical to the level of privacy concern experienced by consumers. Sheehan and Hoy [48] find information control to be a primary factor in consumers' concern for privacy in an online environment. As discussed previously, there is evidence that trust reduces the level of privacy concern. Consumers who perceive a loss of information control in personalized online interactions are likely to feel vulnerable. They must depend on the benevolence and competence of online entities to responsibly use and protect the consumer's personal information. For these consumers, trust in the online entity is likely to be more influential in reducing privacy concern, compared to consumers who perceive higher levels of information control and are less vulnerable to the

online firm's intentions and abilities. Thus, we expect an interaction effect in which increasing levels of information control will weaken the effect of trust on the level of privacy concern.

SDI-based personalization relies on information that consumers have actively provided to the firm, so not only have these consumers consciously chosen to provide personal information, but they are explicitly aware of the exchange of information. However, NSDI-based personalization uses information collected without the knowledge or permission consumers, so they may not be aware that an exchange of information has even taken place.

H3: Increasing levels of information control will weaken the effect of trust on privacy concern.

Malhotra, Kim and Agarwal [32] view online privacy concern as consisting of three dimensions – collection, control and awareness – grounded in social contract theory. They note that social contract theory requires "the rights of exit and voice" as components of norm-generating social contracts [12]. NSDI is collected and used without the consumer's awareness, consent or control. Consumers whose privacy concerns are higher may see this as a violation of the implicit social contract between themselves and the marketer. It is at this point that they may exercise their rights of exit and voice by leaving the relationship and/or spreading negative word-of-mouth. Thus we expect the level of perceived information control will decrease the negative effect of privacy concern on behavioral intentions.

H4: Increasing levels of information control will weaken the effect of privacy concern on behavioral intentions.

2.6 Moderating effects of compensation

Compensation may be offered in one of two forms – cash or non-cash. *Cash compensation* is defined as currency or currency-equivalent rewards, such as gifts or discounts on future purchases. For instance, the Sheehan and Hoy [48] study used the gift of a mousepad as

compensation. Cash compensation provides the consumer with an explicit, tangible benefit that figures into the privacy calculus. Conversely, *non-cash compensation* is defined as a benefit that has no cash-equivalent value, such as information, assistance or customization. For example, online shoppers are apparently willing to have their behaviors watched if it is used to customize their shopping experience [19].

Trust and privacy concern. As previously discussed, a key dimension of trust is the perceived benevolence of the other party. By offering the customer a benefit, whether in the form of a tangible cash reward or intangible non-cash reward, a firm may signal its benevolence to the consumer. Trust "is about expectations of the future … It accrues to individuals and organizations due to their previous good works and clear promises" [50, p. 58]. Thus, the firm's offer of compensation in either form may increase the effect of the consumer's level of general trust by providing an example of a "good work" and making an implicit promise of future benefits.

H5: A personalized non-cash compensation offer strengthens the relationship between trust and privacy concern.

H6: A personalized cash compensation offer strengthens the relationship between trust and privacy concern.

Privacy concern and behavioral intentions. Previous research conceptualizes the relationship between consumers and direct marketers as a social contract in which consumers expect to receive compensation (e.g., coupons, special offers) for providing personal information used for direct mail purposes [31, 37]. To enter into such contracts, consumers must first perceive the benefits to outweigh the costs. While consumers desire the benefits of personalized offers, they do not want to sacrifice privacy [37]:

> If they perceive (consciously or unconsciously) that the social or economic gain ... outweighs the attendant reduction in privacy, they will participate in the contract. Otherwise, they will not. (p. 208)

Sheehan and Hoy [48] test this proposition by examining the effect of compensation on online privacy concern. They find consumers' willingness to exchange personal information for compensation to be a significant factor in reducing the effects of online privacy concern. They conclude that online consumers appear to be willing to sacrifice some degree of privacy in order to gain something of value in the exchange. Their finding resonates with Westin's [57] observation that consumers often consider the nature of the benefit offered in exchange for information when deciding if their privacy has been violated.

A personalized cash compensation offer strengthens the relationship between trust and privacy concern.

H7: A personalized non-cash compensation offer weakens the relationship between privacy concern and behavioral intentions.

H8: A personalized cash compensation offer weakens the relationship between privacy concern and behavioral intentions.

3. Method

3.1 Design and sample

A 2 (NSDI, SDI) x 3 (control, non-cash compensation, cash compensation) between-subjects experiment was used to collect data for the tests of hypotheses. Participants were university undergraduates at a large, public university located in the southwestern United States who were awarded class credit for participation. The sample included more males (56%) than females (44%) and the average age was 21 years. Some marketing research cautions against the use of student samples [42]; however, undergraduate students represent a significant percentage of online consumers [23]. Indeed, 96% of participants in this study reported everyday use of the

Internet and 86% had made five or more online purchases. In addition, the context of this study – online travel purchasing – is one that is familiar to this demographic group. Travel and airline tickets represent 29 percent of the more than $2.9 billion spent online by college students, more than double the next highest category of spending [52].

3.2 Procedure

We developed a Web site to simulate a personalized interaction during the online purchase of airline tickets. The site was pre-tested with a convenience sample of graduate students to discover and correct any issues with the functionality of the simulation. Participants in the main study were told that the research would ask for their opinions about the features of a proposed travel Web site targeted to college students; hence, they were not aware of the purpose of the experiment. Instructors provided the Web site URL and directed students to visit the site within a prescribed time period to register. During registration, participants' demographic data were collected and the trust scale was administered.

Within 48 hours following registration, participants received an email that contained a username and password along with instructions to revisit the Web site and select "I already have a user ID and password" to begin the simulation. After logging in, they were asked to book a trip to a favorite destination and then complete a brief online survey about the booking experience. During the simulated booking process, an animation was displayed that depicted information flowing between two computers, along with this statement: "We are matching your social security number and credit card information with our affiliates' records." Then a message window appeared with a personalized message. The simulation and survey took about 15 minutes.

3.3 Manipulations

To simulate the use of non-self-disclosed information (NSDI) and self-disclosed information (SDI), personal information was collected from participants in two ways. One group submitted information in the first week of the term on student information forms that were routinely requested by instructors at the start-up of a course. In addition to their names, contact information, previous coursework and work history, students reported three items of personal information: their favorite fast-food restaurant, favorite musical group and the make and model of their automobile. Near the end of the term – approximately 90 days later – instructors invited students to participate in the research project in exchange for extra credit. The time lag increased the likelihood that students would not recall having provided the personal information earlier in the term that was subsequently used in the experiment. The second group was asked to disclose the same three items of personal information during the booking process. As a check on the manipulation, participants were asked to report their level of agreement (Strongly Disagree=1 to Strongly Agree=7) with the following statement: "I have no idea how this Web site collected my personal information." The mean scores for the NSDI and SDI group were significantly different (4.63 and 4.25, respectively; difference =.38; $p<.03$).

To examine the effects of compensation offers, participants were randomly assigned to one of three conditions. In the control condition, a pop-up window provided information about an upcoming concert by the participant's favorite musical group. In the non-cash compensation condition, the pop-up offered a discount coupon at the participant's favorite fast-food restaurant. In the cash compensation condition, participants were presented with a $20 cash voucher at their favorite fast-food restaurant.

<Tables 1 and 2 about here>

3.4 Measurement and data analysis

Constructs were measured using seven-point Likert-type scales. Items are provided in Table 1 along with standardized loadings, composite reliabilities and average variances extracted. Items from Dinev and Hart's [10] scale for online privacy concern were adapted for this study. Items used to measure trust, behavioral intentions and information control were adapted from the work of Liu, Marchewka and Ku [30].

Structural equation modeling (SEM) using maximum likelihood estimation was used to examine measurement properties of the scales and to test hypothesized relationships among constructs. SEM permits the simultaneous estimation of multiple regression equations in a path model, such as the one proposed in this study. Multi-group analyses, described in detail subsequently, were used to test hypothesized moderating effects.

Reliability and validity of the scales were evaluated in a confirmatory factor analysis in which the four reflective first-order latent constructs (i.e., Trust, Privacy Concern, Behavioral Intentions, and Information Control) were allowed to freely correlate. The CFA provided evidence for a close fit between the measurement model and the data (χ_2=146, df = 84, RMSEA = .043, CFI = .99). Reliability was assessed by examining item and construct reliability (Peter, 1981). All item loadings were significant ($p < .01$) and at or above the recommended .60 parameter value. Construct reliability was evaluated by examining composite reliability (CR) and average variance extracted (AVE) [1]. All constructs were well above the recommended threshold of .60 for CR. Similarly, all constructs were above the threshold of .50 for AVE.

Discriminant validity was tested by comparing the shared variance among indicators of a construct (i.e., AVE) with the variance shared between constructs (i.e., correlations). The test for discriminant validity is met when the square root of AVE for the construct is greater than

correlations with other constructs [15]. Table 2 displays correlations between constructs, with the square root of AVE for each construct on the diagonal. Reading down the columns and/or across the rows, the square root of AVE for each construct is greater than the correlations between constructs, meeting the test for discriminant validity. Descriptive statistics are also provided in Table 2.

In the following sections, we report the results of hypotheses tests and discuss the findings. Path coefficients, significance of the coefficients and results of hypotheses tests are summarized in Table 3.

<Tables 3 and 4 about here>

4. Results

The baseline structural model was a close fit with the data ($\chi 2$=61, df=42, p=.027, RMSEA=.034, CFI=.996, GFI=.974). The relationship between trust and privacy concern was significant and negative (.-15, p<.01), supporting H1. Similarly, the relationship between privacy concern and behavioral intentions was significant and negative (-.33, p<.01), in support of H2.

Multi-group analyses were used to test the moderating effects of information control proposed by Hypotheses 3 and 4 and compensation offers proposed by Hypotheses 5 – 8. For the test of perceived information control, two groups were formed by splitting the sample at the mid-point of the information control scale (i.e., 4.0 on a 7-point scale). Thus participants who scored below 4.0 (n=266) were classified as low information control and those who scored at or above 4.0 (n=128) were included in the high information control group. The mean scores for the low information control group (2.63) and the high information control group (5.35) were significantly different (p<.001). For the test of

compensation offers, the three compensation conditions were used to classify participants: Group 1 – Control; Group 2 – Non-cash Compensation, and; Group 3 – Cash Compensation.

We tested for configural and measurement equivalence to establish construct validity and reliability across groups before examining structural differences proposed by the hypotheses [55]. Results of these tests are summarized in Table 4. The unconstrained baseline models (i.e., Models 1a, 2a and 3a) were a close fit with the data sets, providing evidence for configural equivalence. Measurement equivalence was evaluated by examining the statistical significance of the difference in the fit between the unconstrained baseline models and models that constrained item loadings to equality across groups (i.e., Models 1b, 2b and 3b). The unconstrained and constrained models in all three multi-group analyses were not significantly different, which indicated measurement equivalence across the groups.

For the information control groups, the model that constrained the Trust → Privacy Concern path weight to equality across groups (Model 1c) was not significantly different (p>.95) for the low (-.14, p<.01) and high (-.15, p<.01) information control groups. Therefore, this path is not moderated by information control, and H3 is not supported. However, the model that constrained the Privacy Concern → Behavioral Intentions path weight to equality (Model 1d) was significantly different (p<.001). For the low information control group, privacy concern exerted a strong negative influence on behavioral intentions (-.46, p<.001). For the high information control group, privacy concern had no significant effect on behavioral intentions (p>.58). Thus increasing levels of information control weaken the effect of privacy concern on behavioral intentions, as proposed by H4.

In the tests of compensation offers, the model that constrained the Trust → Privacy Concern path weight to equality across the control and non-cash compensation groups (Model 2c) was significantly different (p<.01). For the non-cash compensation group, trust had a negative influence on privacy concern (-.22, p<.001). For the control group, trust had no significant effect on privacy concern (p>.32). Thus an offer of non-cash compensation strengthens the attenuating effect of trust on privacy concern, as proposed by H5. In contrast, the model that constrained the Privacy Concern → Behavioral Intentions path weight to equality (Model 2d) was not significantly different (p>.91) for the control (-.39, p<.001) and non-cash compensation groups (-.41, p<.001). Therefore H6 is not supported.

Similarly, the fit of the model that constrained the Trust → Privacy Concern path weight to equality across the control and cash compensation groups (Model 3c) was significantly different (p<.03). For the cash compensation group, trust had a negative influence on privacy concern (-.22, p<.001). Again, trust had no significant effect on privacy concern (p>.32) for the control group. Results support H7; that is, an offer of cash compensation strengthens the attenuating effect of trust on privacy concern. The model that constrained the Privacy Concern → Behavioral Intentions path weight to equality (Model 3d) was not significantly different (p>.78) for the control (-.36, p<.001) and cash compensation groups (-.41, p<.001). Therefore H8 is not supported.

7. Discussion

The aim of this research was to explore the potential moderating effects of compensation and information control on the relationships between trust, privacy concern and behavioral intentions in the context of personalized online interactions. To this end, we first replicated

previous research testing the effects of trust on privacy concern and privacy concern on behavioral intentions as a baseline condition. Consistent with previous research, trust reduced privacy concern, and privacy concern had a negative influence on behavioral intentions.

Next, we examined the potential moderating effects of information control. Findings show that the level of information control has no effect on the negative relationship between generalized online trust and privacy concern. There was no significant difference between the low-control condition and the high-control condition. However, the effect of privacy concern on behavioral intentions was significantly different between the low-control and high-control groups. When information control is low (i.e. the firm has collected and used personal information about the consumer without his or her awareness and consent), the negative relationship between privacy concern and behavorial intentions is significantly stronger.

Finally, we examined the moderating effects of compensation, which yielded mixed results. As proposed in previous research, the compensation offer weakened the effect of trust on privacy concern. Participants may have invoked a "privacy calculus," making trust less salient to privacy concern when a cash or non-cash compensation offer was made. An alternative explanation is that participants perceived the offer of compensation as a signal of the firm's benevolence resulting in higher expectations of positive future outcomes. Interestingly, the same effect did not hold for the relationship between privacy concern and behavioral intentions. There was no significant difference in this relationship between the control group and participants in either the cash or non-cash compensation condition. These findings have practical and theoretical implications, which are discussed in the following sections.

7.1 Managerial implications

This study confirms that trust is a significant factor in reducing privacy concern. Managers who are interested in reducing consumers' privacy concerns are advised to take steps to build trust with consumers. For example, managers should provide privacy, security, good online experience, and trustworthy quality of information [21]. Further, firms can enhance trust when firms rely on social cues to communicate the firm's reputation in the market place [8, 26].

Our findings suggest that using NSDI to personalize online interactions may be risky. The majority of participants in Study 2 (55 percent) perceived the use of NSDI. When participants perceived the use of NSDI, trust did not reduce privacy concern. Consequently, managerial actions that aim to build trust will be ineffective for reducing this group's privacy concerns. Furthermore, the perception of NSDI significantly increased the negative effect of privacy concern on behavioral intentions. These consumers are less likely to engage in desirable behaviors, such as being loyal to the firm and engaging in positive word-of-mouth behaviors.

Additionally, findings suggest that the offer of personalized compensation may not be an effective tool for managing consumers' privacy concerns. The offer of compensation reduced the influence of trust on privacy concern to non-significance. We attribute this outcome to the consumer's privacy calculus whereby privacy is sacrificed to gain the benefit of compensation. Surprisingly, the offer of compensation strengthened the negative effect of privacy concern on behavioral intentions. Hence, it appears that compensation offers do not mitigate the negative effect of privacy concern on behavioral intentions.

7.2 Theoretical contributions

The concept of non-self-disclosed information (NSDI) was introduced and tested in this study. This concept is particularly relevant to understanding the tension between privacy concern and personalization of online interactions. While current literature explains consumers'

willingness to self-disclose information, it offers little insight into the effects of using the increasing volume of personal information that is collected without the consumer's knowledge and consent. This research provides evidence that the use of NSDI to personalize customer interactions has undesirable consequences. In addition, the study investigates the limitations of a compensation offer as a potential tool for mitigating the negative effects of privacy concern in online personalization.

As with any research design, trade-offs were made in order to address our research objectives. The limitations of this study point to interesting directions for further research. First, the sample was restricted to college students to control for the potential influence of demographic factors and, therefore, results may not be generalizable to other populations. Conducting similar experiments with a representative sample of online shoppers would permit the exploration of the effects of key demographic characteristics such as age, income, education and online experience. In addition, a different research design could more closely model "real world" behavior. For example, participant observation combined with phenomenological interviews may provide insight into additional variables that are relevant to privacy concern that were not considered in this study. Finally, this research was conducted in the context of a service, that is, online travel booking. Results could be different in other contexts, such as services that require more sensitive information (i.e., banking, insurance) or involve the purchase of goods.

Findings also suggest the need for further research. While the majority of participants detected the use of NSDI, a significant minority (45 percent) were relatively unaware of its use. It would be interesting to explore consumers' awareness thresholds for NSDI. When are consumers likely to detect the use of NSDI? Does it depend on the sensitivity of the information

that is used? It appeared that the offer of cash compensation may have raised awareness of the use of NSDI. What types of personalization trigger the detection of NSDI use?

The use of non-self-disclosed information has implications not only for firm behavior, but also for public policy. From a firm's perspective, the use of non-self disclosed information may not yield the desired results. However, firms must encourage consumers to directly provide information and educate consumers on how their personal information is utilized to enhance their online experience. For example, Meinert et al. [35] demonstrated that a consumer's willingness to provide information to online firms increased as the level of privacy guaranteed by the privacy policy statements increased. When firms educated consumers regarding the level of privacy promised in privacy statements, consumers' willingness to provide personal information increased. From a public policy perspective, firms must be required to disclose and educate consumers on how personal information is gathered and used through the firm's privacy policy statements.

Table 1
Measures

Construct	Items	Loading
	Anchors: Strongly Disagree (1) - Strongly Agree (7)	
Trust		
CR = .96	▪ I trust travel websites to make an effort to keep my personal information out of the hands of unauthorized individuals.	.91
AVE = .85	▪ I trust travel websites not release personal information about me without my express permission.	.93
	▪ I trust travel websites to take care of my personal information.	.97
	▪ Overall, travel websites are trustworthy.	.87
Privacy Concern	▪ I would be concerned that information collected about me by a website like this could be misused.	.75
CR = .92	▪ I would be concerned that credit card information used for purchases on a website like this could be stolen while being transferred.	.84
AVE = .75	▪ I would be concerned about the privacy of personal information about me collected on a website like this.	.96
	▪ I would be concerned that personal information about me collected on a website like this could be used in a way I did not foresee.	.91
Behavioral Intentions	▪ I would use this website in the future to book online travel.	.94
	▪ I would recommend this website to my friends.	.97
CR = .95	▪ I have positive things to say about this website.	.88
AVE = .86		
Information Control	▪ I was informed about the personal information this website would collect about me.	.75
CR = .90	▪ This website explained why personal information was being collected.	.92
AVE = .68	▪ This website explained how personal information collected about me would be used.	.90
	▪ This website gave me a clear choice before using personal information about me.	.71

CR = Composite reliability; AVE = Average variance extracted

Table 2
Data Distributions, Correlations [a] and Discriminant Validity

Construct	Mean	SD	TR	PC	INTENT	INFCTL
Trust (TR)	4.69	1.43	**.92**			
Privacy Concern (PC)	4.66	1.51	-.15	**.87**		
Behavioral Intentions (INTENT)	4.32	1.61	.19	-.33	**.93**	
Information Control (INFCTL)	3.51	1.58	.08 [ns]	-.14	.62	**.83**

SD=standard deviation; Square root of AVE in bold on the diagonal
[a] Correlations significant at $p<.01$ unless otherwise noted
[ns] Not significant at $p<.05$

Table 3
Parameter Estimates and Results of Hypotheses Tests

	Hypotheses	Estimate	*p*-value	Results
H1	Trust → Privacy Concern	-.15	<.01	*Supported*
H2	Privacy Concern → Behavioral Intentions	-.33	<.01	*Supported*
Moderating effects of perceived information control				
		Low (High)		
H3	Trust → Privacy Concern	-.14 (-.15)	*ns*	*Not Supported*
H4	Privacy Concern → Behavioral Intentions	-.46 (*ns*)	<.01	*Supported*
Moderating effects of compensation				
		Control		
	Trust → Privacy Concern	*(Compensation)*		
H5	Non-cash compensation	*ns* (-.22)	<.01	*Supported*
H6	Cash compensation	*ns* (-.22)	<.03	*Supported*
		Control		
	Privacy Concern → Behavioral Intentions	*(Compensation)*		
H7	Non-cash compensation	-.39 (-.41)	*ns*	*Not Supported*
H8	Cash compensation	-.36 (-.41)	*ns*	*Not Supported*

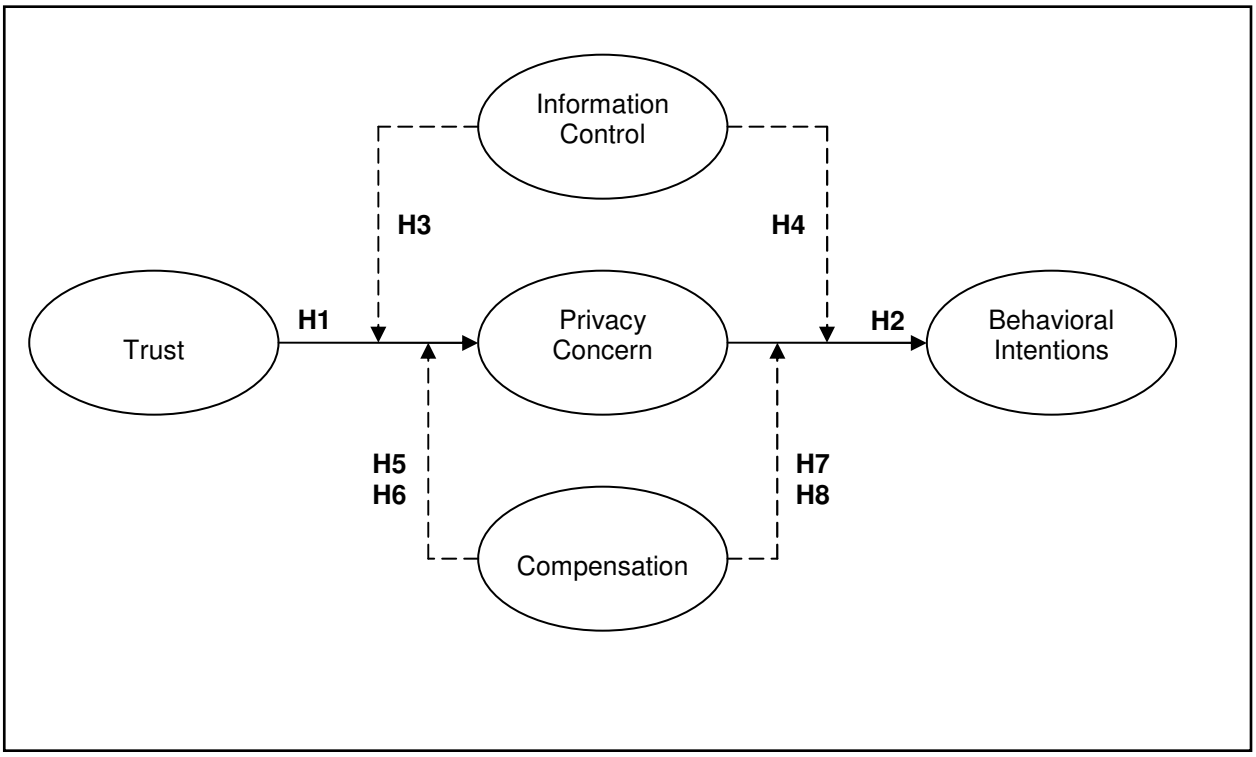
ns = not significant at $p<.05$

Table 4
Tests of Configural and Measurement Invariance for Multi-Group Analyses

	Model Description	RMSEA[a]	CFI[b]	$\chi 2$	*df*	$\Delta\chi 2$	Δdf	*Statistical Significance*[c]
	Information Control							
1a	Unconstrained baseline model	.038	.989	131	84	----	----	----
1b	Model 1a with factor loadings constrained to equality	.036	.989	139	92	8	8	*p>.41*
1c	Model 1b with Trust → Privacy Concern constrained	.036	.989	139	93	0	1	*p>.95*
1d	Model 1b with Privacy Concern → Behavioral Intentions constrained	.042	.985	156	93	17	1	*p<.01*
	Non-Cash Compensation							
2a	Unconstrained baseline model	.033	.990	112	84	----	----	----
2b	Model 2a with factor loadings constrained to equality	.033	.991	119	92	7	8	*p>.55*
2c	Model 2b with Trust → Privacy Concern constrained	.036	.989	125	93	6	1	*p<.01*
2d	Model 2b with Privacy Concern → Behavioral Intentions constrained	.032	.991	119	93	0	1	*p>.91*
	Cash Compensation							
3a	Unconstrained baseline model	.000	.999	76	84	----	----	----
3b	Model 3a with factor loadings constrained to equality	.000	.999	84	92	8	8	*p>.48*
3c	Model 3b with Trust → Privacy Concern constrained	.000	.999	89	93	5	1	*p<.03*
3d	Model 3b with Privacy Concern → Behavioral Intentions constrained	.000	.999	84	84	1	1	*p>.73*

[a]Root Mean Squared Error of Approximation
[b]Comparative Fit Index
[c]Significance of $\Delta\chi 2$

Figure 1
Conceptual Model



REFERENCES

1. Bagozzi, R. P. & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, 16(1), 74.
2. Bowlby, J. (1969). *Attachment and loss: Vol. I. Attachment*. New York: Basic Books.
3. Castañeda, J. & Montoro, F. (2007). The effect of internet general privacy concern on customer behavior. *Electronic Commerce Research*, 7(2), 117-141.
4. Chellappa, R. K. & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, 6(2-3), 181-202.
5. Coner, A. (2003). Personalization and customization in financial portals. *Journal of American Academy of Business, Cambridge*, 2(2), 498.
6. Coviello, N., Milley, R. & Marcolin, B. (2001). Understanding it-enabled interactivity in contemporary marketing. *Journal of Interactive Marketing*, 15(4), 18-33.
7. Culnan, M. J. & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, 10(1), 104-115.
8. De Laat, P. B. (2005). Trusting virtual trust. *Ethics and Information Technology*, 7, 167-180.
9. Dinev, T. & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, 10(2), 7-29.
10. Dinev, T. & Hart, P. (2006). Privacy concerns and levels of information exchange: An empirical investigation of intended e-services use. *E - Service Journal*, 4(3), 25-57.
11. Doney, P. M. & Cannon, J. P. (1997). An examination of the nature of trust in buyer-seller relationships. *Journal of Marketing*, 61(2), 35-51.
12. Dunfee, T. W., Smith, N. C. & Ross Jr, W. T. (1999). Social contracts and marketing ethics. *Journal of Marketing*, 63(3), 14-32.
13. Eastlick, M. A., Lotz, S. L. & Warrington, P. (2006). Understanding online b-to-c relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, 59(8), 877-886.
14. Fishbein, M. & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, Mass.: Addison-Wesley.
15. Fornell, C. & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research (JMR)*, 18(1), 39-50.
16. Garbarino, E. & Johnson, M. S. (1999). The different roles of satisfaction, trust, and commitment in customer relationships. *Journal of Marketing*, 63(2), 70.
17. Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing*, 10(1), 149-166.
18. Graeff, T. R. & Harmon, S. (2002). Collecting and using personal data: Consumers' awareness and concerns. *The Journal of Consumer Marketing*, 19(4/5), 302.
19. Greenberg, P. A. (2000). E-shoppers choose personalization over privacdy. *e-Commerce Times*, January 4 edition.
20. Gwinner, K. P., Gremler, D. D. & Bitner, M. J. (1998). Relational benefits in services industries: The customer's perspective. *Academy of Marketing Science. Journal*, 26(2), 101.

21. Ha, H.-Y. (2004). Factors influencing consumer perceptions of brand trust online. *The Journal of Product and Brand Management*, 13(4/5), 329.
22. Hoffman, D. L., Novak, T. P. & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM*, 42(4), 80-85.
23. Horrigan, J. (2008). Internet users like the convenience but worry about the security of their financial information. www.pewinternet.org. Accessed July 17, 2008.
24. Jacobs, R. S., Hyman, M. R. & Mcquitty, S. (2000). Exchange-specific self-disclosure, social self-disclosure, and personal selling. *American Marketing Association. Conference Proceedings*, 11, 261.
25. Jarvenpaa, S. L., Knoll, K. & Leidner, D. E. (1998). Is anybody out there? *Journal of Management Information Systems*, 14(4), 29-64.
26. Kim, M.-S. & Ahn, J.-H. (2006). Comparison of trust sources of online market-maker in the e-marketplace: Buyer's and seller's perspectives. *Journal of Computer Information Systems*, 47(1), 84-94.
27. Koballa, T. R. (1988). The determinants of female junior high school students' intentions to enroll in elective physical science courses in high school: Testing the applicability of the theory of reasoned action. *Journal of Research In Science Teaching*, 25(479-492.
28. Langenderfer, J. & Cook, D. L. (2004). Oh, what a tangled web we weave: The state of privacy protection in the informatino economy and recommendations for governance. *Journal of Business Research*, 57(7), 734.
29. Liu, C., Marchewka, J. T. & Ku, C. (2004). American and taiwanese perceptions concerning privacy, trust, and behavioral intentions in electronic commerce. *Journal of Global Information Management*, 1(1), 18-40.
30. Liu, C., Marchewka, J. T., Lu, J. & Chun-Sheng, Y. (2005). Beyond concern a privacy-trust-behavioral intention model of electronic commerce. *Information & Management*, 42(2), 289-304.
31. 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.
32. Malhotra, N. K., Kim, S. S. & Agarwal, J. (2004). Internet users' information privacy concerns (iuipc): The construct, the scale and a causal model. *Information Systems Research*, 15(4), 336-355.
33. Mangalindan, M. (2003). Web ads on the rebound. *Wall Street Journal*, August 25 edition.
34. Mascarenhas, O. A. J., Kesavan, R. & Bernacchi, M. D. (2003). Co-managing online privacy: A call for joint ownership. *Journal of Consumer Marketing*, 20(7), 686-702.
35. Meinert, D. B., Peterson, D. K., Criswell, J. R. & Crossland, M. D. (2006). Privacy policy statements and consumer willingness to provide personal information. *Journal of Electronic Commerce in Organizations*, 4(1), 1-17.
36. Milne, G. R. (2000). Privacy and ethical issues in database/interactive marketing and public policy: A research framework and overview of the special issue. *Journal of Public Policy & Marketing*, 19(1), 1-6.
37. Milne, G. R. & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing*, 12(2), 206-215.
38. Moon, Y. (2000). Intimate exchanges: Using computers to elicit self-disclosure from consumers. *Journal of Consumer Research*, 26(4), 323.

39. Moorman, C., Deshpande, R. & Zaltman, G. (1993). Factors affecting trust in market research relationships. *Journal of Marketing*, 57(1), 81-101.
40. Morgan, R. M. & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *Journal of Marketing*, 58(3), 20-38.
41. Nowak, G. J. & Phelps, J. (1995). Direct marketing and the use of individual-level consumer information: Determining how and when "Privacy" Matters. *Journal of Direct Marketing*, 9(3), 46-60.
42. Peterson, R. A. (2001). On the use of college students in social science research: Insights from a second-order meta-analysis. *Journal of Consumer Research*, 28(3), 450-461.
43. Phelps, J. E., D'souza, G. & Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing*, 15(4), 2-17.
44. Postma, O. J. & Brokke, M. (2002). Personalisation in practice: The proven effects of personalisation. *Journal of Database Marketing*, 9(2), 137.
45. Prosser, W. L. (1960). Privacy. *California Law Review*, 48(3), 383.
46. Sackmann, S., Struker, J. & Accorsi, R. (2006). Personalization in privacy-aware highly dynamic systems. *Communications of the ACM*, 49(9), 32-38.
47. Sheehan, K. B. (2002). Toward a typology of internet users and online privacy concerns. *Information Society*, 18(1), 21-32.
48. Sheehan, K. B. & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, 19(1), 62-73.
49. Sheppard, B. H., Hartwick, J. & Warshaw, P. R. (1988). The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research. *Journal of Consumer Research*, 15(3), 325-343.
50. Shneiderman, B. (2000). Designing trust into online experiences. *Communications of the ACM*, 43(12), 57-59.
51. Smith, R. & Shao, J. (2007). Privacy and e-commerce: A consumer-centric perspective. *Electronic Commerce Research*, 7(2), 89-116.
52. Student Monitor. (2004). Spring 2004 lifestyle & media report. Proprietary marketing study of college students' activities and interests.
53. Van Dyke, T. P., Vishal, M. & Nemati, H. (2007). The effect of consumer privacy empowerment on trust and privacy concerns in e-commerce. *Electronic Markets*, 17(1), 68-81.
54. Van Slyke, C., Shim, J. T., Johnson, R. & Jiang, J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, 7(6), 415-443.
55. Vandenberg, R. J. & Lance, C. E. (2000). A review and synthesis of the measurement invariance literature: Suggestions, practices, and recommendations for organizational research. *Organizational Research Methods*, 3(1), 4-70.
56. Warren, S. V. & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193-220.
57. Westin, A. F. (1997). Legal safeguards to insure privacy in a computer society. *Communications of the ACM*, 10, 533-537.
58. Zucker, L. G. (1986). Production of trust: Institutional sources of economic structure: 1840-1920. In Staw, B. M. C., Larry L. (ed.), *Research in organizational behavior* (pp. 53-111). Greenwich, CT: JAI Press.