Association for Information Systems
AIS Electronic Library (AISeL)

ICIS 2007 Proceedings

International Conference on Information Systems (ICIS)

December 2007

Understanding Online Information Disclosure As a Privacy Calculus Adjusted by Exchange Fairness

Rathindra Sarathy
Oklahoma State University

Han Li
Oklahoma State University

UNDERSTANDING ONLINE INFORMATION DISCLOSURE AS A PRIVACY CALCULUS ADJUSTED BY EXCHANGE FAIRNESS

Han Li
Virginia State University
Department of Computer Information Systems
Petersburg, VA 23806
hli@vsu.edu

Rathindra Sarathy
Oklahoma State University
Department of Management Science & Information Systems
Stillwater, OK 74075
rathin.sarathy@okstate.edu

Abstract

Current studies on information privacy fail to explain widely observed contradictions between online consumers' privacy concern (treated as a general personality trait) and online information disclosure. These contradictions occur because situation-specific factors are not taken into account. This paper contributes to the literature on information privacy by theorizing and empirically testing how information disclosure is driven by competing situation-specific benefits and risk factors. The results of this study indicate that, in the context of an e-commerce transaction with an unfamiliar vendor, information disclosure is the result of competing influences of exchange benefits and two types of privacy beliefs (privacy protection belief and privacy risk belief). In addition, the effect of monetary rewards is dependent upon the fairness of information exchange. Monetary rewards could undermine information disclosure when information collected has low relevance to the purpose of the e-commerce transaction.

Keywords: Privacy belief, online information disclosure, exchange benefits, fairness of information exchange

Introduction

Based on statistics provided by the U.S. Department of Commerce for the first quarter of 2005, the retail value of e-commerce is $19.8 billion and growing rapidly. Accompanying this growth is the increasing tension between companies' need to gather and analyze consumer data and consumers' need for information privacy. Consumers' personal information is a valuable asset to online companies. Companies rely on consumers' personal information not only to enable basic transactions and operations of their business but also to identify new business opportunities. For example, companies cross sell products based on consumers' browsing pattern or explicitly collected preference information. On the other hand, online shoppers are increasingly concerned about their information privacy. 85 percent of online users have declined to give out personal information to websites at one time or another; and 34 percent have lied about their personal habit and preference information (Teltzrow and Kobsa 2004). The tension between online vendors' need for information and consumers' desire for information privacy is recognized as a major impediment to the growth of e-commerce. This issue has attracted the attention of researchers trying to have a better understanding about online shoppers' privacy concerns and the impact on their willingness to disclose information (Dinev and Hart 2006; Malhotra et al. 2004).

However, most studies on privacy-related behavior primarily emphasize *privacy concern* (Dinev and Hart 2006; Malhotra et al. 2004; Smith et al. 1996; Stewart and Segars 2002). Privacy concern is defined in these studies as an individual's personality trait or general tendency to worry about information privacy (Malhotra et al. 2004, p 341). These studies have produced inconsistent results regarding the impact of privacy concern. Privacy concern was found to be significant when included as a sole predictor (Smith et al. 1996, Stewart and Segars 2002) and has been found to have a weak or insignificant impact on privacy-related behavior in the existence of situation-specific variables such as trust belief, risk belief, etc. (Malhotra et al. 2004, Awad and Krishnan 2006). Further, current studies on information privacy fail to explain widely observed privacy contradictions found in practice between online consumers' privacy concern and online information disclosure. For example, a survey by Acquisti et al. (2005) found that a significant percentage of people with high privacy concern (41 percent) rarely read private policies containing promised rules and safeguards. We argue that various situation-specific factors, such as nature of the information to be collected by the vendor, economic benefits, privacy beliefs formed from the interaction with the websites, among others, should be investigated to have a better understanding of the *privacy contradiction* phenomena. This is consistent with the idea suggested by Laufer and Wolfe (1977) that "Individuals' concepts of privacy are tied to concrete situations in everyday life".

Further, drivers of information disclosure should be examined in the context of an exchange process where consumers make cost-benefit trade-offs to decide whether to exchange their personal information for economic or non-economic benefits (Culnan and Bies 2003). Individuals are more likely to disclose personal information if risks could be offset by benefits. Some researchers have taken an exclusively economic approach in studying factors that entice consumers to disclose information. They argue that personal information is a commodity that can be clearly priced and exchanged using monetary rewards (Hann et al. 2002; Laudon 1996). For example, consumers may release their information to a direct marketing company in exchange for cash.

The pure economic approach to information exchange is arguable in the context of the conventional e-commerce marketplace. First, the information exchange acts as a by-product of a primary exchange where goods or services are exchanged for money or other goods (Culnan and Bies 2003). The successful completion of an ecommerce transaction often requires some consumer information to validate the identity of the consumer and allow normal business operations such as product delivery, customization, etc. Therefore, *consumer information is an essential enabler of ecommerce transactions, rather than being just an exchangeable commodity*. Second, thus far monetary rewards have been primarily examined as an explicit enticer of information disclosure and have been found to increase consumers' willingness to disclose personal information (Hann et al. 2002). However, our approach takes into account the realities of the conventional e-commerce marketplace. Monetary rewards such as discounts or coupons when offered are usually meant to attract online shoppers to complete the exchange for products or services, and *not purely to lure consumers to disclose their personal information*. Third, the information exchange is governed by a *social contract* since consumers "do not view their personal data in the context of an economic exchange" (Hoffman et al. 1999, p130 and p132). and the social contract has an implicit assessment that "their personal information will subsequently be used fairly and they will not suffer negative consequences" (Culnan and Armstrong 1999, p106). The perceived fairness of the information exchange will modify the cost-benefit tradeoff analysis.

The objective of this study is to investigate situation-specific motivators that entice online consumers to disclose personal information and how fairness elements could influence the cost-benefit tradeoff analysis. In particular, our research questions are: 1) How does the perceived fairness of information exchange adjust the cost-benefit tradeoff analysis? 2) What is the impact of monetary rewards on information disclosure? 3) How does perceived fairness of information exchange adjust the impact of monetary rewards?

Literature and Research Hypotheses

Information Exchange and the Privacy Calculus

Information privacy is the ability of individuals to control when, how, and to what extent their personal information is exchanged with and used by others (Culnan and Bies 2003; Stone et al. 1983; Westin 1967). Absolute information privacy is usually not possible. Online shoppers often have to disclose some personal information to complete an ecommerce transaction. Consumers' willingness to disclose their personal information must be situated in an exchange context to be understood (Culnan and Bies 2003). Consumers often make cost-benefit trade-offs to decide whether to exchange their personal information for economic or non-economic benefits. The benefits are balanced against risks of information disclosure. Individuals are more likely to disclose personal information if the risks of privacy could be offset by benefits. Such cost-benefit analysis is part of the "privacy calculus" that drives the decision on whether to disclose information or not (Culnan and Bies 2003, p.327). Until now, only a few studies have empirically studied online privacy in the context such a privacy calculus (Dinev and Hart 2006).

Information Exchange and Social Contract

In the context of conventional e-commerce marketplace, information disclosure can be considered a type of non-monetary exchange governed by an implicit social contract (Culnan and Bies 2003). Social Contract Theory (SCT) has been applied in the context of marketing to explain the exchange relationship between a firm and its customers (Dunfee et al. 1999). The major assumption of SCT is bounded moral rationality, i.e. "individual moral agents lack the information, time, and emotional strength to make perfect judgments" (Donaldson and Dunfee 1994; Dunfee et al. 1999, p18). This assumption matches the context of this study, i.e. initial information disclosure with during an ecommerce transaction with an unfamiliar vendor, where the information exchange is especially susceptible to bounded moral rationality. Online shoppers often do not have complete information to make correct judgments about unfamiliar websites and the information exchange could incur unknown consequences.

One of the core principles of SCT is that "norm-specifying microsocial contracts must be grounded in informed consent buttressed by a right of exit" (Donaldson and Dunfee, 1994). This implies that the information exchange is based on shared understanding or *norms* about information exchange and parties involved in exchange have a right to withdraw from the transaction. Culnan and Bies (2003) have done an excellent job of integrating the concept of social contracts and justice theory to examine consumer privacy and proposed three justice principles underlying norms of a social contract that governs information exchange. The central theme of these justice principles is *exchange fairness*. Based on this, it can be said that the cost-benefit analysis or privacy calculus is subject to a second assessment about whether the information is collected fairly and will subsequently be used fairly i.e., the fairness-based social contract (Culnan and Bies 2003; Laufer and Wolfe 1977).

Research Model

In this study, information privacy is examined as part of an exchange process governed by a social contract. The research model (discussed below – Figure 1) depicts how online shoppers' intention to disclose their personal information is driven by competing assessments of situation-specific exchange benefits and exchange risks adjusted for fair information practices. The model suggests that consumers' willingness to disclose personal information could be enhanced in three ways: 1) providing sufficient benefits such as attractive products or services, discounts, etc; 2) reducing privacy-related costs since the invasion to information privacy is the major cost factor of information disclosure by inducing favorable privacy protection belief or perceptions, and reducing unfavorable risk beliefs, and 3) increasing the perceived fairness of information disclosure. The following three subsections illustrate each of the approaches and their impact on behavioral intention to disclose personal information.

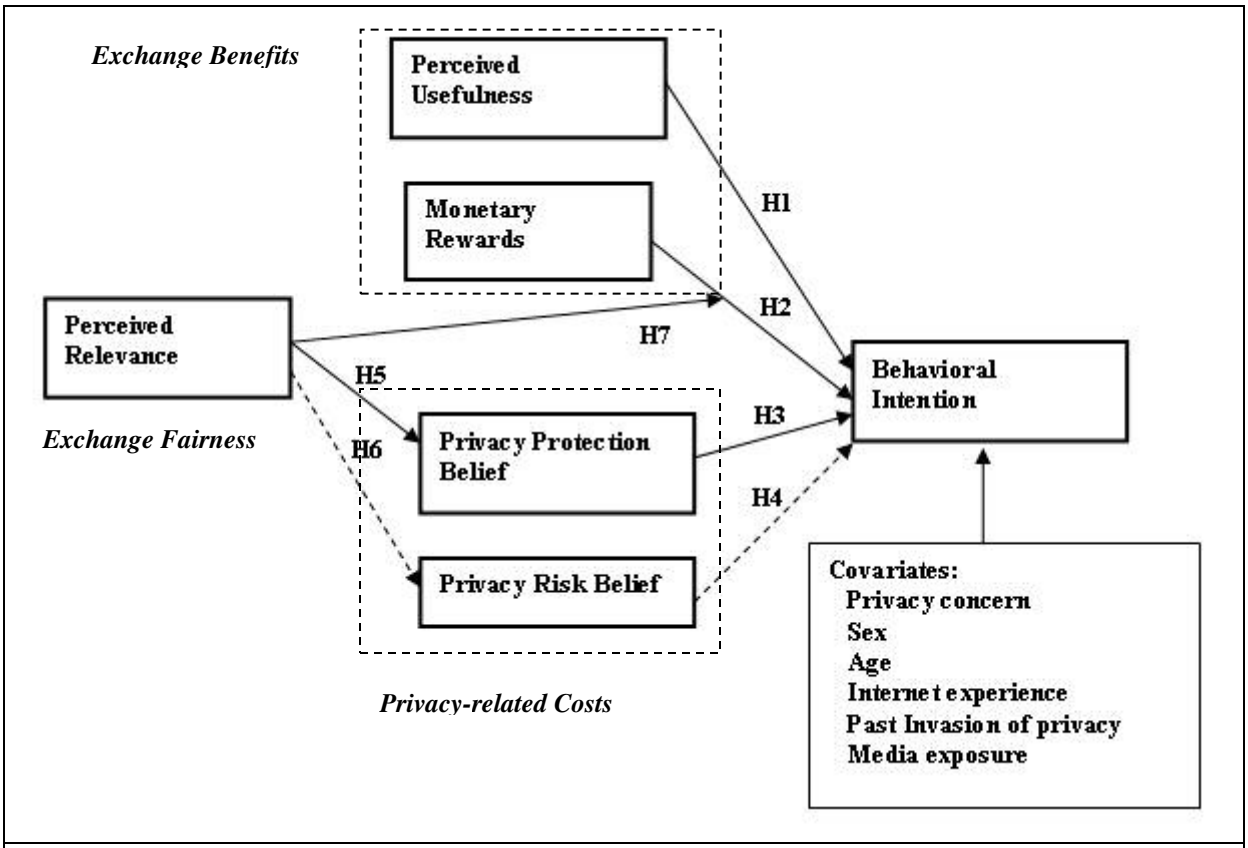

Figure 1. Research Model. Positive effect ⟶, negative effect - - ►.

Exchange Benefits

For an initial e-commerce transaction with an unfamiliar vendor's website, the attractiveness of the products or services is probably the foremost factor that drives consumers' willingness to disclose personal information, and information disclosure is only a by-product of completing the transaction. Consumers may evaluate the attractiveness of the products or services based on multiple dimensions such as usefulness, ease of use, fun, etc. In this study, we tested our research model using an internet-based fax service, which is one type of information technology (IT). Based on the rich literature of technology acceptance model (TAM), perceived usefulness is one of the most important dimensions that determine the behavioral intention to adopt a technology (Davis 1989). Therefore, in this study, attractiveness of the offering is operationalized as perceived usefulness of the products or services. Examining other dimensions is beyond the scope of this study. Since information exchange is an enabler for the primary exchange of money for products or services (Culnan and Bies 2003), the usefulness of the products or services should increase online shoppers' willingness to relinquish some privacy in return for the utility from the products or services. Therefore, we hypothesize:

H1: Perceived usefulness of the product or service has a positive impact on online shoppers' behavioral intention to disclose their personal information.

Information disclosure could also be driven by other benefits such as monetary rewards, time saving, etc. Monetary rewards are important motivators that lead to information disclosure and are used by many Internet businesses (Hui et al. 2006; Phelps et al. 2000). However, unlike previous studies where monetary rewards are empirically investigated as explicit monetary benefits obtained in return for personal information, we assume, based on a

conventional e-commerce marketplace, that monetary rewards are not exchanged explicitly for information. Instead, money rewards are manipulated as benefits to attract customers to purchase products or services. Since information disclosure is the by-product of the primary exchange of products/services for money, monetary rewards are hypothesized to take a similar positive effect on information disclosure.

H2: Monetary rewards have a positive impact on online shoppers' behavioral intention to disclose their personal information.

Exchange Risks (Privacy-related Costs)

Many risks could be involved in an e-commerce transaction such as poor product quality, unauthorized sharing of personal information, among others. In this study, our focus is on privacy risks. Two privacy beliefs could be formed from the assessment of privacy risks: privacy protection belief and privacy risk belief. The former refers to the subjective probability that consumers believe that their private information is protected as expected (Metzger 2004; Pavlou and Chellappa 2001). The latter is defined as the expected loss potential associated with releasing personal information to the firm (Malhotra et al. 2004). These two contrary privacy beliefs reflect different aspects of risk assessment and their separation may allow us examine the privacy calculus more closely. These two privacy beliefs, while related may be driven or shaped by different factors and perhaps play different roles in influencing privacy decisions or behaviors. Although privacy protection belief is not related to the explicit benefits of the primary exchange, consumers with a high privacy protection belief should perceive more control over privacy risks and are more likely to disclose their personal information. Conversely, consumers with high privacy risk beliefs should perceive a greater loss potential and may be wary about disclosing their personal information. Therefore,

H3: Privacy protection belief has a positive impact on online shoppers' behavioral intention to disclose their personal information.

H4: Privacy risk belief has a negative impact on online shoppers' behavioral intention to disclose their personal information.

Fairness of Information Exchange

As discussed earlier, besides cost-benefit tradeoffs, information disclosure in the online environment is further subject to perception about the fairness of information disclosure. The perceived fairness of disclosure pertains to whether the collection of certain information and the subsequent usage are fair relative to the context of exchange. Fairness perception is especially important in an online environment since it involves greater uncertainty about the vendor's information practice. For example, online vendors could surreptitiously collect point-click data without the consumers' explicit permission that, when combined with data collected from the e-commerce transaction, can be used to profile online shoppers and perform price discrimination.

Online firms could implement fair information practices to enhance perceived fairness and alleviate the effect of privacy risks on consumers' willingness to disclose personal information (Culnan and Armstrong 1999; Culnan and Bies 2003). Internet users are generally concerned about the amount of information collected by an online vendor, their ability to control over the collected information and their awareness of how the collected information is used (Malhotra et al. 2004). Among these three sub-dimensions of information privacy concern, collection is "the central theme of equitable information exchange" (Malhotra et al. 2004). Collected information should be commensurate with the exchange benefits. It implies that the nature of information requested should be *relevant*. Therefore, in this study, perceived fairness of information exchange is operationalized as perceived relevance of information, which is defined as the "the degree to which the data requested appear relevant or appear to have a bearing upon the purpose of the inquiry" (Stone 1981). Online shoppers could rely on the relevance of information as a signal about the potential privacy risks. A website collecting information relevant to the transaction would be deemed more likely to respect and protect consumers' information privacy. On the other hand, a website requesting irrelevant information would be considered more likely to violate information privacy through surreptitious use of the information for unauthorized purposes. Therefore, we hypothesize:

H5: Perceived relevance of information collected has a positive impact on privacy protection belief.

H6 Perceived relevance of information collected has a negative impact on privacy risk belief.

Besides the effect on privacy perceptions, the fairness of information exchange could also adjust the effect of monetary rewards. For example, consumers may undervalue the monetary compensation offered in exchange for personal information if companies collect information irrelevant to the purpose of the transaction.

H7: The relationship between monetary rewards and intention to disclosure information is moderated by relevance of information, such that the positive impact is stronger when perceived relevance is high.

Covariates

Besides the five situation-specific factors in our model that could influence the primary exchange (of money for goods or services) and information disclosure, we also consider the impact of various individual differences on information disclosure. For example, older consumers, female consumers and those who have been victims of privacy invasion and/or exposed to negative media exposure about information privacy are more likely to be concerned about privacy (Campell 1997; Milne and Rohm 2000). These personal difference factors are included as control variables in our research model since they are situation-independent and are not the focus of this study. Specifically, a total of six personal difference factors that might influence privacy decisions/behaviors were included as control variables for predicting intention to disclose personal information. They are gender, age, Internet experience, previous experience of being victims of privacy invasion, media exposure of privacy invasion incidents and privacy concern. Among the six covariates, privacy concern has been the most examined in prior literature with inconsistent results. For example, privacy concern was found to be significant when included as a sole predictor (Smith et al. 1996; Stewart et al. 2002) and was often found to exert weak influence or no influence over information disclosure in the existence of other predictor such as trust belief, risk belief, etc (Awad and Krishnan 2006; Malhotra et al. 2004). In the presence of multiple situation-specific factors included in our research model, the direct effect of privacy concern on behavioral intention is expected to be unstable. Even if some weak direct relationship is found, such relationship has limited external validity. So, privacy concern is included as a control variable.

Research Methodology

Study Design and Procedures

An artificial website that mimics a real commercial website providing internet fax service was created for the purposes of this study. Besides easy manipulation, an artificial website also helps to rule out the effect of store familiarity and reputation since our research focus is on initial information exchange or for unfamiliar website. The other variables were measured directly without manipulation.

Monetary rewards were manipulated at two levels: no reward and reward ($10 off the service fee for two months or a total of $20 discount). Subjects were randomly assigned to only one of these two treatment conditions, i.e. either no reward or reward. A major task page was used to introduce the task scenario to subjects and to provide detailed step by step instructions. Each subject assumed the role of an online shopper searching for electronic fax service to be used to fax resumes for job hunting. Subjects were requested to interact with the website as naturally as possible to get to know the company and the service offered by the company. Then, they were instructed to evaluate a membership sign-up form which is required before using the company's internet fax service. All experimental subjects were exposed to the same membership sign-up form requesting name, gender, e-mail address, postal address, phone number, credit card information, secret question, and date of birth. After evaluating the sign-up form, subjects were required to fill out the survey.

Variable Measurement

Existing published scales were adapted to measure variables in the research model whenever possible. Some items were re-worded slightly to reflect the research context[1]. The perceived usefulness scale was adapted from TAM model by Davis et al (1989). The general term "task" was replaced with more specific phrases as "send/receive my documents" or "job search". Perceived relevance items were modified from Stone (1981). The original scale consists of one item "Information collected by others should appear relevant to the purpose for which it is collected". To increase the internal reliability of this instrument, the single item was re-worded into three items that match our research context. They are: 1) "Information gathered seemed relevant for member registration"; 2) "Questions in the signup form appeared to have a bearing upon the purpose of the signing up"; 3) "Information collected in the sign-up form looks appropriate for signing up for the program". Privacy protection belief was measured using the scales by Pavlou and Chellappa (2001). Privacy risk belief was adapted from the instruments by Malhotra et al (2004). The terms "online firms" and "the information" were replaced with more specific terms as "this vendor" and "my personal information". Behavioral intention to disclose personal information was measured using scales by Malhotra et al. (2004) and MacKenzie and Spreng (1992). Privacy concern consisted of three items developed by Malhotra et al (2004) for measuring global information privacy concern. The detailed privacy concern scale developed by Malhotra et al (2004) was not used in this study because the focus of this study is not on the sub-dimensions of privacy concern. All constructs are measured on a seven-point Likert scales with 1 being "strongly disagree" and 7 being "strongly agree". All these instruments were found to be reliable and valid and the detailed results are given in the Data Analysis section. In addition, a single question (whether the website provided discounts or coupons for signing up with its service) was developed to check whether the manipulation on monetary rewards was successful.

Survey Administration

Before the final experiment, a pilot study was administered to 75 undergraduate and graduate students in a major Midwestern U.S. university. The purpose was to evaluate the content validity and clarity of measurement scales. In the final experimental study, the recruitment message was delivered to about 238 undergraduate students who are different from those in the pilot study. The participation was voluntary. Extra credit accounting for less than 2% of their total grade was used as an incentive for participation. A total of 182 valid responses were received. The demography of survey respondents is given in Table 1.

Table 1. Demography Distribution of Survey Respondents

Gender		Age	
Male	66.5%	19-25	94.5%
Female	33.5%	26-30	3.8%
		31-35	1.1%
Internet Experience		>35	0.5%
<1 yr	11.6%		
1-3 yr	39.8%		
3-6 yr	33.1%		
>=6 yr	15.5%		

[1] A copy of the study's instrument is available from the authors on request.

Data Analysis

The t-test on monetary reward manipulation was significant with a p-value <0.01, suggesting that the manipulation of monetary rewards was successful. Partial least squares (PLS) technique was then applied to test the measurement model and research hypotheses. PLS requires a sample size that is at least ten times larger than the number of paths going to an endogenous construct when all constructs are reflective (Chin 1998). For our research model, the maximum number of path leading to an endogenous variable is twelve including the interaction term between perceived relevance and monetary rewards, and the six control variables. Therefore, a sample size of 182 is sufficient for testing our research model. Furthermore, PLS does not assume a multivariate normal distribution and interval scales, making it appropriate for testing our research model with monetary rewards as a binary manipulated construct.

A two-step approach was adopted to test our research model. We first assessed the reliability and validity of all latent constructs or the measurement model and then tested our research hypotheses or structural model.

Measurement Model

Results of testing the measurement model are presented in Tables 2 and 3. Table 2 provides the composite reliability (CR), average variance extracted (AVE) and loadings of each item on its intended construct and on other constructs (i.e., cross-loadings). A scale is considered as reliable if its composite reliability (CR) is above 0.7 and average variance extracted (AVE) above 0.5 (Bagozzi and Yi 1988). As shown in Table 2, all scales are reliable. For convergent validity, we examined the standardized loadings and their significance. All items load significantly on their respective latent construct and all loadings except PPB5 are above 0.6, the recommended cutoff by Bagozzi and Yi (1988). But, the loading of PPB5 is still above 0.5, which is acceptable according to Chin (1998). Discriminant validity of each latent construct was tested by the method recommended by Fornell and Larcker (1981). The square root of AVE of each construct should be higher than the correlation between that construct and any other constructs. This criterion is satisfied by all latent constructs (Table 3). Overall, these results indicate that our measurement model has adequate convergent and discriminant validity. So, the structural model can be examined further.

Hypotheses Testing Results

Figure 2 summarizes the results of testing the hypotheses. The model could explain 50.8% of the variance in behavioral intention, 16.5% of the variance in privacy protection belief and 9.9% of the variance in privacy risk belief.

We first analyzed the interaction effect or Hypothesis 7, before testing the other hypotheses. To test Hypothesis 7, we followed the procedures proposed by Chin et al. (2003). The existence of interaction was evaluated based on both effect size and statistical significance. The effect size of interaction (f^2) was 0.022, which satisfies the 0.02 cutoff for small effect size (Cohen 1988)[2]. The interaction is also found to be statistically significant ($p < 0.05$). Hence, the perceived relevance of information moderates the relationship between monetary rewards and behavioral intention. The interaction pattern is show in Figure 3, which consists of two regression lines with one for high value of perceived relevance (i.e. one standard deviation above the mean) and one for a low value of perceived relevance (i.e., one standard deviation below the mean). The utility by Preacher et al. (2003) was then implemented to find out the region of statistical significance. We found that when the perceived relevance of information is 4.7 or above, the relationship between monetary rewards and behavioral intention is not statistically significant. When the perceived relevance is below 4.7, the relationship becomes negative and statistically significant ($p < 0.05$). Therefore, H_7 was partially supported. Despite the existence of significant moderation, the interaction pattern is counter-intuitive and will be discussed in the following section.

Because the interaction is significant, main effect H_2 cannot be interpreted. The results of the tests of the other hypotheses H_1, H_3, H_4, H_5 and H_6 were statistically significant. Therefore, the overall research model is well supported except for the unexpected interaction pattern. In addition, none of the six covariates (gender, age, Internet

[2] $f^2 = [R^2 \text{ (interaction model)} - R^2 \text{ (main effects model)}] / [1 - R^2 \text{ (main effects model)}]$.

experience, previous experience of being victims of privacy invasion, media exposure of privacy invasion incidents and privacy concern) were found to be significant, suggesting that situation-specific factors are the major driver for information disclosure and the effects of personal difference factors are overridden by those of salient beliefs.

Table 2. Loadings, Composite Reliability (CR) and Average Variance Extracted (AVE) of measurement instruments

		Loadings					
Constructs/Items		PU	PPB	PRB	RELE	BI	PC
PU	PU1	**0.772**	0.305	-0.200	0.247	0.333	0.048
CR = 0.927	PU2	**0.881**	0.243	-0.194	0.197	0.356	0.059
AVE = 0.717	PU3	**0.883**	0.323	-0.238	0.282	0.405	0.077
	PU4	**0.826**	0.251	-0.185	0.258	0.269	-0.010
	PU5	**0.868**	0.253	-0.252	0.227	0.398	-0.086
PPB	PPB1	0.273	**0.755**	-0.389	0.255	0.472	-0.158
CR = 0.848	PPB2	0.261	**0.779**	-0.409	0.376	0.453	-0.096
AVE = 0.533	PPB3	0.206	**0.801**	-0.427	0.309	0.373	-0.113
	PPB4	0.263	**0.767**	-0.457	0.319	0.398	-0.128
	PPB5	0.187	**0.507**	-0.205	0.188	0.179	-0.105
PRB	PBR1	-0.271	-0.461	**0.880**	-0.224	-0.520	0.277
CR = 0.928	PBR2	-0.234	-0.431	**0.855**	-0.311	-0.462	0.219
AVE = 0.762	PBR3	-0.179	-0.503	**0.898**	-0.271	-0.541	0.317
	PBR4	-0.211	-0.456	**0.858**	-0.292	-0.478	0.252
RELE	Relev1	0.293	0.349	-0.231	**0.877**	0.379	-0.163
CR = 0.909	Relev2	0.158	0.301	-0.258	**0.823**	0.382	-0.184
AVE = 0.769	Relev3	0.292	0.406	-0.328	**0.928**	0.410	-0.200
BI	BI1	0.426	0.513	-0.556	0.391	**0.939**	-0.224
CR = 0.942	BI2	0.359	0.501	-0.510	0.329	**0.899**	-0.151
AVE = 0.803	BI3	0.319	0.450	-0.475	0.415	**0.843**	-0.186
	BI4	0.396	0.449	-0.510	0.463	**0.897**	-0.256
PC	PC1	0.080	-0.131	0.272	-0.173	-0.167	**0.842**
CR = 0.877	PC2	-0.053	-0.155	0.272	-0.180	-0.256	**0.891**
AVE = 0.704	PC3	0.053	-0.116	0.225	-0.176	-0.125	**0.789**

Note: PU = perceived usefulness; PPB = privacy protection belief; PRB = privacy risk belief; RELE = perceived relevance; BI = behavioral intention; PC = privacy concern. Diagonal boldface numbers are loadings (correlations) of indicators to their own construct; other off-diagonal numbers are cross-loadings.

Table 3. Discriminant Validity of Measurement Model						
	PU	PPB	PRB	RELE	BI	PC
PU	**0.847**					
PPB	0.328	**0.730**				
PRB	-0.255	-0.531	**0.873**			
RELE	0.285	0.406	-0.314	**0.877**		
BI	0.421	0.535	-0.574	0.447	**0.896**	
PC	0.017	-0.163	0.306	-0.208	-0.233	**0.839**

Note: Diagonal elements are the square root of the AVE values. Off-diagonal elements are the correlations among latent constructs.

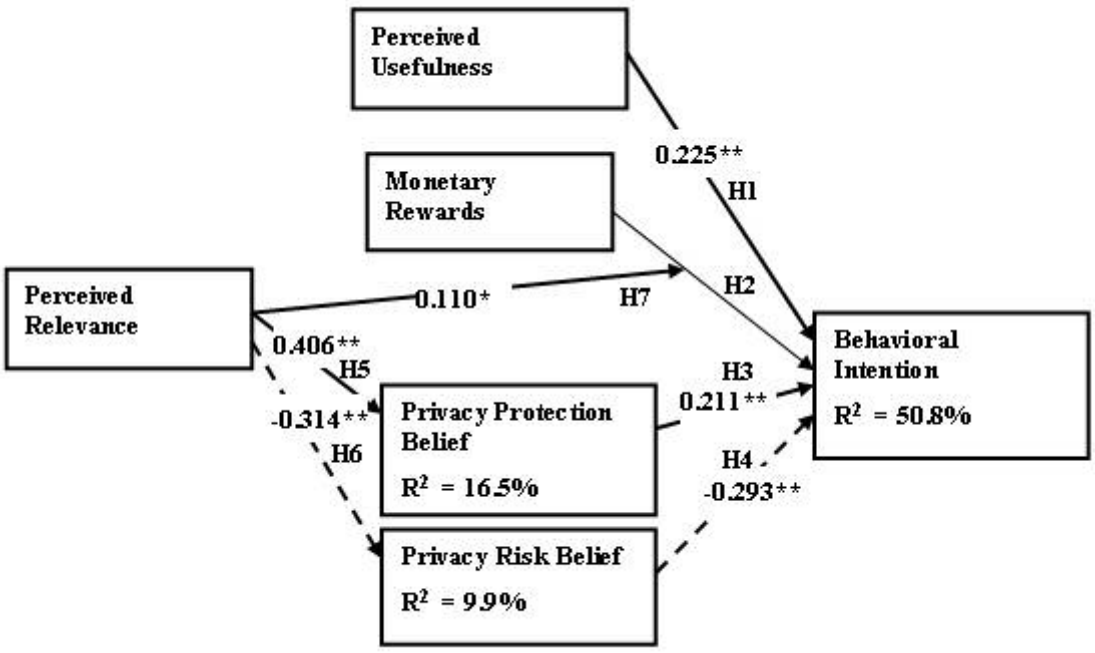

Figure 2. Results of testing hypotheses using PLS analysis. Completely standardized estimates, controlled for covariates in the research model, *p < 0.05, **p < 0.01 (two-tailed).

Discussions

Summary of Findings and Limitations

Our findings suggest that when a product or service is attractive to online shoppers, they are more likely to disclose their personal information. Interestingly, we found that monetary rewards could have a significant undermining effect on willingness to disclose personal information when information collected is perceived to have low to moderate relevance. This implies that monetary rewards, in the presence of low perceived exchange fairness, may actually hold back online shoppers from disclosing their information. The undermining effect of rewards can be

explained using cognitive evaluation theory (Deci and Ryan 1985), which states that such undermining could occur "when events are perceived to be influenced and controlled by extrinsic factors" (such as monetary rewards) (Tietje 2002, p364). Therefore, in our research context, online firms may be viewed unfavorably when they are perceived as attempting to use monetary rewards to influence information disclosure (or membership sign-up) or when online shoppers perceive a salient contingency between monetary rewards and information disclosure. This is consistent with what has been found by Hoffman et al (1999) that "consumers do not view their personal data in the context of an economic exchange." The fairness of information exchange is an important part of the social contract in information disclosure. Collecting improper information is very likely to enhance the salience of the monetary reward's disclosure-contingency and the subsequent undermining effect.

Our results suggest that online shoppers' willingness to disclose personal information is also driven by their salient beliefs regarding the level of privacy protection offered as well as the expected privacy risks associated with releasing personal information involved. The assessment of privacy risks is further adjusted by the perceived fairness of information exchange. Collecting information of high relevance was found to enhance privacy protection belief and reduce privacy risk belief.

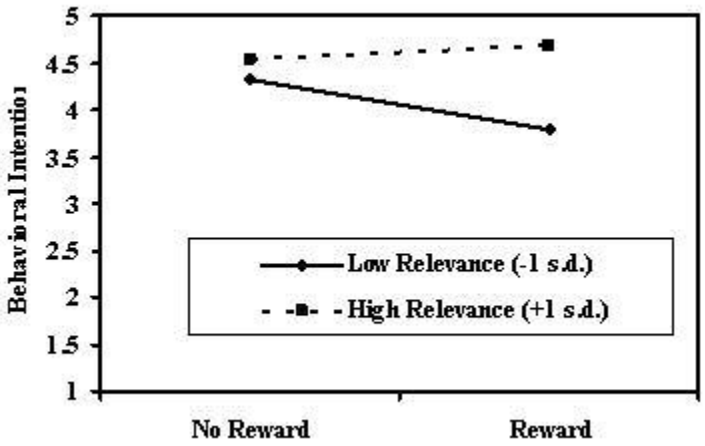

Figure 3. The interaction pattern between monetary rewards and behavioral intention to disclose personal information.

Before we discuss the implications of our study, we point to some of its limitations. Although we found an undermining effect of monetary rewards, we should exercise caution in generalizing it to other contexts. Other situation-specific factors could also influence the monetary rewards' disclosure-contingency and the subsequent undermining effect. For example, website quality may be a factor influencing the undermining effect. A poorly designed website is very likely to make consumers suspicious and trigger the perception about the monetary reward's disclosure contingency and the subsequent undermining effect. In addition, the study uses student subjects. Their age may not be representative of the natural range for common online shoppers. Empirical studies using a different subject population could help to provide stronger support for our findings. However, using student subjects for online shopping tasks may not constitute a major concern for our study. To certain extent, undergraduate students are fairly typical of online consumers as suggested by the result of a recent survey that most of the online shoppers have some college or even high-level education (Lightner 2003). In addition, the tasks used in this study do not require managerial or technical knowledge from subjects. Subjects were just instructed to interact with the experimental website as they normally would to get to know the company and then evaluate the membership sign-up form. All these may help to overcome some of limitations of using student subjects. Another limitation is that our study did not measure actual privacy behaviors. Instead, behavioral *intention* is used as the proxy for actual behaviors. Our approach is consistent with the dominant research practice based on Theory of Reasoned Action (TRA) (Fishbein and Ajzen 1975). According to TRA, behavioral intention was suggested to have close relationship with actual behaviors. But, future studies could be conducted by setting up actual buying scenarios and measuring the actual behavior of giving out personal information to get a more accurate understanding of privacy behaviors.

Implications for Research

The results of this study have five important implications for research. First, willingness to disclose personal information is largely driven by situation-specific factors. Our results are consistent with Laufer and Wolfe (1977) who argued that "Individuals' concepts of privacy are tied to concrete situations in everyday life". This study examined a subset of the situation-specific factors related to the exchange process. Future studies could examine other situation-specific factors such as reputation of the vendor, design of the website, etc.

Second, our findings show that benefits from the primary exchange (money for goods/services) could also influence information disclosure. For example, perceived usefulness, as the benefit of the primary exchange, is found to enhance information disclosure as well. Therefore, when examining initial information disclosure in a conventional e-commerce marketplace, researchers should treat information disclosure as a by-product of the primary exchange of money for products or services and examine the impact of the benefits of the primary exchange on information disclosure as well.

Third, we found that collecting information perceived to have low relevance will enhance the salience of monetary rewards' disclosure-contingency, which then leads to the undermining effect of monetary rewards on information disclosure. The effect of monetary rewards could also be moderated by other factors in a business context such as the design of a website, reputation of the vendor, offering time of the reward, etc. Future studies are needed to have better understanding of the effect of monetary rewards or other explicit benefits.

Fourth, our findings support the premise that information disclosure involves a cost-benefit tradeoff analysis inherent in the privacy calculus. Privacy risks are evaluated against exchange benefits. Willingness to disclose personal information is driven by the competing influences of exchange benefits and the two contrary privacy beliefs. Attractive benefits from the primary exchange by themselves, or together with high privacy protection belief, could override the influence of privacy risks and result in high behavioral intention to disclose personal information. Future studies are needed to examine the effectiveness of various types of benefits and privacy protection belief in overriding the effect of privacy risk belief more closely. Under what condition will certain benefits be more effective than other benefits? What factors help to enhance privacy protection belief and/or reduce privacy risk belief? In this study, we investigated the effect of perceived relevance of information collected on these two opposing privacy beliefs. Other factors could also exert influence over these two contrary privacy beliefs such as emotional response to a website, privacy policy, third-party seals, etc.

Finally, the results of this study support the argument that the cost-benefit tradeoff analysis involved in information disclosure is affected by the assessment of fairness of the information exchange. Perceived fairness of information exchange is found to enhance privacy protection belief, reduce privacy risk belief and moderate the impact of monetary rewards. Therefore, social contract theory provides a useful theoretical foundation for researchers to understand information disclosure in conventional marketplace.

Implications for Practice

The findings of this study also have important implications for online vendors that collect personal information in order to enable e-commerce transactions. First, online vendors should understand that the benefits offered during the primary exchange may influence information disclosure as well. They should exercise care to ensure that only relevant information is collected. A monetary reward offered to influence the primary exchange may have an adverse effect on information disclosure, when information collected is perceived as irrelevant.

In addition, information disclosure entails inherent privacy risks to online shoppers. Their willingness to disclose personal information is the result of competing influence of exchange benefits and the two contrary privacy beliefs. The effect of privacy risk belief could be overridden by the other factors. Online vendors could enhance consumers' willing to disclose personal information by providing attractive exchange benefits and/or enhancing privacy protection belief.

Besides exchange benefits and privacy risks, online vendors also need to take into account the fairness of information exchange. Online firms could implement fair information practices to boost fairness perception, which further adjusts the cost-benefit tradeoff analysis in information disclosure, i.e. enhancing privacy protection belief, and reducing privacy risk belief. The net result of such adjustment will be online shoppers' greater behavioral intention to disclose their personal information.

Conclusions

This paper contributes by increasing our theoretical and empirical understanding of the effect of situation-specific factors on online shoppers' willingness to disclose their personal information in the context of conventional marketplace. This paper investigated information disclosure as a privacy calculus governed by a social contract to account for not only the cost-benefit tradeoff among competing factors but also the adjustment by the fairness of information disclosure. Willingness to disclose personal information is found to be driven by competing influences of the exchange benefits and two contrary privacy beliefs. Attractive benefits of the primary exchange by themselves or together with high privacy protection belief could override the influence of privacy risks and result in high behavioral intention to disclose personal information. In addition, the study illustrates that the effect of monetary rewards is moderated by perceived relevance of information collected. Monetary rewards could undermine information disclosure.

References

Awad, N.F., and Krishnan, M.S. "The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization," *MIS Quarterly* (30:1) 2006, pp 13-28.

Bagozzi, R.P., and Yi, Y. "On the Evaluation of Structural Equation Models," *Journal of the Academy of Marketing Science* (16:1) 1988, pp 74-94.

Campbell, A. J. "Relationship marketing in consumer markets: a comparison of managerial and consumer attitudes about information privacy," *Journal of Direct Marketing* (11:3) 1997, pp 44-57.

Chin, W.W. "The Partial Least Squares Approach for Structural Equation Modeling," in: *Modern Methods for Business Research,* G.A. Marcoulides (ed.), Lawrence Erlbaum, Mahway, New Jersey, 1998, pp. 295-336.

Chin, W.W., Marcolin, B.L., and P.R. Newsted "A Partial Least Squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic mail adoption study," *Information Systems Research* (14:2) 2003, pp 189-217.

Cohen, J. *Statistical Power Analysis for the Behavior Sciences*, (2nd edition ed.) Lawrence Erlbaum, Hillsdale, NJ, 1988.

Culnan, M.J., and Armstrong, P.K. "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation," *Organization Science* (10:1) 1999, pp 104-115.

Culnan, M.J., and Bies, R.J. "Consumer privacy: Balancing economic and justice consideration," *Journal of Social Issues* (59:2) 2003, pp 323-342.

Deci, E.L., and Ryan, R.M. *Intrinsic Motivation and Self-Determination in Human Behavior*. New York, Plenum 1985.

Davis, F.D. "Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology," *MIS Quarterly* (13:3 (September)) 1989, pp 319-340.

Dinev, T., and Hart, P. "An extended privacy calculus model for e-commerce transactions," *Information Systems Research* (17:1) 2006, pp 61-80.

Donaldson, T., and Dunfee, T.W. "Toward a unified conception of business ethics: integrative social contracts theory," *Academy of Management Review* (19:2) 1994, pp 252-284.

Dunfee, T.W., Smith, N.C., and Ross, W.T., "Social contracts and marketing ethics," *Journal of Marketing* (63 (July)) 1999, pp 14-32.

Fishbein, M. and Ajzen, I. *Belief Attitude, Intention, and Behavior: An Introduction to Theory and Research. Reading*, MA., Addison-Wesley, 1975.

Fornell, C., and Larcker, D. "Evaluating structural equation models with unobservable variables and measurement error," *Journal of Marketing Research* (18) 1981, pp 39-50.

Hann, I.H., Hui, K.L., Lee, T.S., and Png, I.P.L. "Online information privacy: measuring the cost-benefit trade-Off," Proceedings of the Twenty-Third Annual International Conference on Information Systems, Barcelona, Spain, 2002, pp. 1-10.

Hoffman, D.L., Novak, T.P., and Peralta, M.A. "Information privacy in the marketspace: Implications for the commercial uses of anonymity on the Web," *Information Society* (15:2) 1999, pp 129-139.

Hui, K.L., Tan, B.C.Y., and Goh, C.Y. "Online information disclosure: motivators and measurements," *ACM Transactions on Internet Technology* (6:4), November 2006, pp 415-441.

Laudon, K.C. "Markets and privacy," *Communications of the ACM* (39:9) 1996, pp 92-104.
Laufer, R.S., and Wolfe, M. "Privacy as a concept and a social issue: A multidimensional development theory," *Journal of Social Issues* (33:3) 1977, pp 22-42.
Lightner, N.J. "What users want in e-commerce design: effects of age, education and income," *Ergonomics* (46:1-3), 2003, pp 153
Malhotra, N.K., Kim, S.S., and Agarwal, J. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4) 2004, pp 336-355.
Metzger, M.J. "Privacy, trust, and disclosure: exploring barriers to electronic commerce," *Journal of Computer-Mediated Communication* (9:4) 2004.
Milne, G.R. and Rohm, A.J. "Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives." *Journal of Public Policy Marketing* (19:2) 2000, pp 238-249.
Pavlou, P.A., and Chellappa, R.K. "The Role of Perceived Privacy and Perceived Security in the Development of Trust in Electronic Commerce Transactions," Marshall School of Business, USC, Los Angeles.
Phelps, J., Nowak, G., and Ferrell, E. "Privacy concerns and consumer willingness to provide personal information," *Journal of Public Policy Marketing* (19:1) 2000, pp 27-41.
Preacher, K.J., Curran, P.J., and Bauer, D.J. "Probing interactions in multiple linear regression, latent curve analysis, and hierarchical linear modeling Interactive calculation tools for establishing simple intercepts, simple slopes, and regions of significance," 2003. http://www.psych.ku.edu/preacher/interact/index.html Last accessed in March, 2007
Stone, D.L. "The effects of the valence of outcomes for providing data and the perceived relevance of the data requested on privacy-related behaviors, beliefs and attitudes," Purdue University, 1981.
Stone, E.F., Gueutal, H.G., Gardner, D.G., and McClure, S. "A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations," *Journal of Applied Psychology* (68:3) 1983, pp 459-468.
Teltzrow, M., and Kobsa, A. "Impacts of user privacy preferences on personalized systems: A comparative study. ," in: *Designing Personalized User Experiences in eCommerce,* C.M. Karat, J. Blom and J. Karat (eds.), Kluwer Academic Publishers, Dordrecht, Netherland, 2004, pp. 315-332.
Tietje, B.C. "When do rewards have enhancement effects? An availability valence approach," *Journal of Consumer Psychology* (12:4) 2002, pp.363-373.
Venkatesh, V., Morris, M.G., Davis, G.B., and Davis, F.D. "User acceptance of information technology: toward a unified view," *MIS Quarterly* (27:3) 2003, pp 425-478.
Westin, A.F. *Privacy and Freedom* Atheneum, New York, 1967.