Understanding situational online information disclosure as a privacy calculus

ACCEPTED BY JOURNAL OF COMPUTER INFORMATION SYSTEMS

Han Li*
School of Business
Minnesota State University Moorhead
Moorhead, MN 56563
Tel: +1 218 477 4067
Fax: + 218 477 2238
Email: li@mnstate.edu

Rathindra Sarathy
Department of Management Science & Information Systems
Spears School of Business
Oklahoma State University
Stillwater, OK 74075
Tel: +1 405 744 8646
Fax: + 405 744 5180
Email: rathin.sarathy@okstate.edu

Heng Xu
College of Information Sciences and Technology
Penn State University
University Park, PA 16802
Tel: +1 814 867 0469
Fax: + 814 865 6426
Email: hxu@ist.psu.edu

Li, H., Sarathy, R., and Xu, H. (2010). "Understanding Situational Online Information Disclosure as a Privacy Calculus," *Journal of Computer Information Systems*, accepted.

Understanding situational online information disclosure as a privacy calculus

ABSTRACT

The effect of situational factors is largely ignored by current studies on information privacy. This paper theorized and empirically tested how an individual's decision-making on information disclosure is driven by competing situational 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, Information disclosure, Exchange benefits, Fairness of information exchange

INTRODUCTION

Public opinion polls and academic surveys reveal that consumers are increasingly concerned about merchants having excessive access to their personal information [45, 47]. Scholars in information systems have examined online privacy issues related to the collection and use of personal information in many different contexts such as privacy responses to general online companies [11, 27], online purchasing [48], Internet banking [49], e-government service [16]. A general understanding from this stream of research is that Internet users with high levels of privacy concerns would perceive high privacy risk and resist disclosing their personal information to those online firms [11].

Most privacy studies primarily emphasize *general privacy concern*, i.e. not specific to a particular website or online company. While such general privacy concerns have received attention as a determinant of privacy-related behaviors within the IS field, legal and social scholars have noted recently that it is important to conceptually and operationally draw a distinction between *general* concerns for privacy and *situation specific* concerns [4, 28, 40]. Bennett [4] indicated that the privacy implications of specific situations or domains can mean something different to everyone. Malhotra et al. [27, p. 349] also acknowledges such contextual emphasis and suggests scholars begin to unravel the intricacies of privacy concerns.

Following the call for the contextual emphasis of privacy research, we argue that various situational factors at a specific level should be investigated to have a better understanding of an individual's decision-making on information disclosure. These situational factors include the type of information to be collected by the vendor, economic benefits, privacy perceptions formed from interaction with a specific website, among others. In this research, we argue that the effect

of general privacy concern is very likely to be overridden by various situational factors at a specific level, i.e. related to a specific online vendor.

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 [8]. 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 [18, 24]. 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 for three reasons. First, for a typical e-commerce transaction in the conventional e-commerce marketplace, the information exchange acts as a by-product of a primary exchange of goods or services for money or other goods and is referred as "second exchange" [8]. 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 a commodity exchangeable with money*. Second, in 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*. Current literature has examined monetary rewards as an explicit enticer of information disclosure outside the context of conventional marketplace and concluded that such

rewards increase consumers' willingness to disclose personal information [18, 21]. It is not clear whether the role of monetary awards stays the same in a conventional marketplace as that in a non-conventional marketplace. Third, the information exchange in conventional marketplace is governed by a *social contract* in which personal information cannot be clearly priced. Consumers "do not view their personal data in the context of an economic exchange" [19]. A social contract involves an implicit assessment of exchange fairness, i.e. the degree of fairness of information exchange involving whether their personal information is collected fairly and, will subsequently be used fairly [7, 8]. *The perceived fairness of the information exchange can modify the cost-benefit tradeoff analysis, i.e. privacy calculus.*

The objective of this study is to investigate situational motivators at a specific level that entice online consumers to disclose personal information to unfamiliar online vendors in a conventional e-commerce marketplace 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 associated with primary exchange on information disclosure? 3) How does perceived fairness of information exchange adjust the impact of monetary rewards?

THEORETICAL FOUNDATION

Online shoppers' privacy behavior follows a "calculus of behavior" [25], influenced jointly by competing benefit and cost factors. One factor may override the effect of another. For example, the urgent need for a spare appliance part (usefulness of the product) may overcome the fear of privacy risks, especially when there are a limited number of vendor choices. Further, information exchange is governed by a social contract or shared *implicit* norms about exchange fairness. Exchange fairness is likely to adjust the pattern of competing relationships among

factors involved in the privacy calculus. In the following sections, we first discuss the information exchange as a "calculus of behavior" involving the evaluation of contrary exchange benefits and risks. Then, we further elaborate information exchange as governed by a social contract.

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 [8, 44, 50]. During information exchange, consumers' privacy behaviors are driven by a privacy calculus [8]. A privacy calculus is a cost-benefit tradeoff analysis that accounts for inhibitors and drivers that simultaneously influence the decision on whether to disclose information or not [8, 11]. Consumers, when requested to provide personal information to corporations, would perform a cost-benefit analysis to assess the outcomes they would face in return for the information, and respond accordingly. The concept of privacy calculus could potentially advance our understanding of complex privacy decisions and behaviors by examining contrary factors at the same time [11].

Although this concept is intuitively appealing, limited studies have *empirically* tested the proposition of a privacy calculus [10, 11]. Dinev and her colleagues proposed and tested a general privacy calculus model consisting of competing influences of benefit and risks of e-commerce transactions [10, 11]. Their focus was on online shoppers' *general* behavioral intentions to submit personal information over the Internet but not in a *specific* information exchange context between a vendor and an online shopper. The context of the information exchange is important for understanding consumers' willingness to disclose their personal information [8, 51]. Privacy behaviors are a result of situational and context-specific cost-benefit analysis of information disclosure [51]. To capture the specific context of the primary exchange

for products or services, our study aimed to understand privacy calculus in the context of a typical e-commerce transaction with an unfamiliar Web site. Specifically, *we considered costs and benefits factors involving both the primary exchange (for products or services) and the second exchange (for information).* As information exchange is only a by-product of e-commerce transaction, it is necessary to consider the tight coupling of the primary exchange and second exchange. It is very likely for benefits or risks of the primary exchange to factor into online shoppers' privacy calculus decision. The impact of benefits of the primary exchange such as product attractiveness may override that of privacy risks.

Information exchange and social contract

At the same time, it is important to recognize that information disclosure decisions involve more than the cost-benefit trade-off analysis discussed in the above section. Information exchange entails considerable uncertainty or is subject to opportunistic behaviors of retailers. For example, without the awareness of the customers, the vendor may use the data collected for purposes other than those stated during data collection. The exact consequences of disclosing personal information may be difficult to determine in advance. Therefore, at least part of the information exchange is not regulated by an *explicit* legal contract. Instead, information exchange in the context of conventional e-commerce marketplace can better be considered as a type of non-monetary exchange governed by an *implicit* social contract [8].

A social contract essentially consists of shared norms between two parties regarding the rights and responsibilities of both parties [13]. Social Contract Theory (SCT) has been applied in the context of marketing to explain the exchange relationship between a firm and its customers. 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" [12, p18]. This is also true

of information disclosure during an e-commerce 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. Therefore, the information exchange is governed by an implicit social contract instead of an explicit legal contract.

Culnan and Bies [8] integrated the concept of social contracts and justice theory and proposed three justice principles underlying norms of a social contract that governs information exchange, namely, distributive justice, procedural justice and interactional justice. The central theme of these justice principles is *exchange fairness*. The cost-benefit trade-off analysis (or privacy calculus) is further adjusted by consumers' understanding or implicit assessment about the fairness of information exchange [8]. Therefore, exchange fairness should be considered a key social norm governing the social contract underlying online information exchange. Consequently, the social contract may be considered violated by an online shopper if a Web site collects information irrelevant to the purpose of the information transaction or benefits of the primary exchange, or if the Web site does not provide an opt-out option when collecting irrelevant personal information, among others. So, a consumer may overestimate the privacy costs of information exchange or underestimate the exchange benefits if the information collected by a vendor is not fair or irrelevant to the purpose of the transaction. 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, constituting a fairness-based social contract [8, 25].

From the above, we can conclude that consumers are likely to perform multiple joint tests before they disclose their information to proceed with further processing of the initial transaction

with unfamiliar online vendors. Online shoppers assess whether the benefits of the exchange are attractive to them, whether costs involved in the exchange process can be justified by benefits to be received and, perhaps more important for information disclosure, whether information disclosure is fair. Each of the tests may be the primary driver of an initial e-commerce transaction. For example, the benefits from the products or services may override the effect of exchange costs and exchange fairness if there are a limited number of alternatives. To get the products or services, customers may have to surrender their privacy even if the online vendor requests irrelevant information. A failure of any of these assessments may cause online shoppers to avoid or terminate transactions with online vendors.

RESEARCH MODEL

In the above section, we proposed that information disclosure is governed by a fairness-based social contract. The social contract involves not only a cost-benefit analysis but also an assessment about exchange fairness and its further adjustment on the cost-benefit analysis. Based on this, the research model (discussed below – Figure 1) is proposed to depict how online shoppers' information disclosure intention is driven by competing assessments of exchange benefits and privacy costs adjusted for exchange fairness.

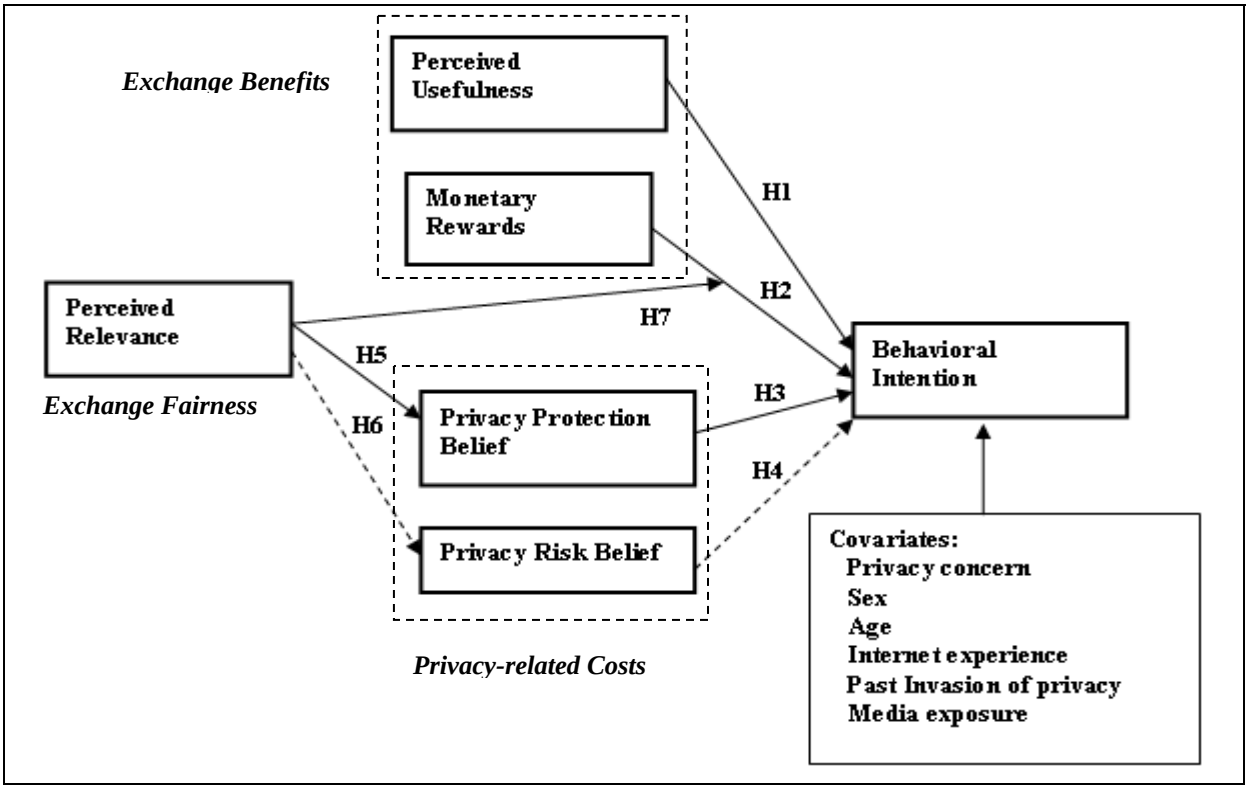

Figure 1: Research Model. Positive effect ⟶, negative effect - - ▸.

Exchange benefits

For an e-commerce transaction with an unfamiliar website, the attractiveness of the products or services is probably the foremost factor that drives consumers' willingness to disclose personal information. 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 and fun. In this study, we tested our research model using an Internet-based fax service, which is one type of information technology. Perceived usefulness is one of the most important dimensions that determine the behavioral intention to adopt a technology [9] and has been found to influence online shoppers' intention to purchase and give out their personal information [15]. Therefore, in this study, attractiveness of the offering is operationalized as perceived usefulness of the products or services. To the extent that

the anticipation of benefits provides direction for actual behavior through energizing and motivating individuals and enhancing the perceived value of various outcomes, a higher expectation about usefulness of the product or service will amplify the desire to engage in the target behavior. Since information exchange is an enabler for the primary exchange of money for products or services [8], 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,

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

Besides perceived usefulness, information disclosure could also be driven by monetary rewards, which are used by many Internet businesses [20, 21, 37]. Money rewards, in this study, are manipulated as benefits to attract customers to purchase products or services, i.e. *benefits of the primary exchange*. Information disclosure, as the enabler for the primary exchange, is a necessity to receive the benefits of the primary exchange [17]. Money rewards add to the total benefits of the primary exchange, which may also increase online shoppers' willingness to disclose their personal information. Therefore,

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

Privacy-related costs

In this research, we propose that two privacy-related costs could be formed from the assessment of outcomes of information disclosure: 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 [30, 35]. The latter is defined as the expected loss potential

associated with releasing personal information to the firm [27]. These two contrary privacy beliefs reflect different aspects of privacy cost 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 information disclosure and are more likely to disclose their personal information. Therefore,

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

A number of privacy studies have empirically verified the negative effect of perceived privacy risk on willingness to disclose personal information in Internet transactions [11, 27, 48]. Consumers may not want to disclose personal information if they sense that their personal information is not effectively protected and there exist high risks of privacy invasion. Therefore,

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 additionally subject to perception about the fairness of information disclosure. Fairness of information exchange is defined as the fair information practice principles or FIP principles [8, 34], pertaining to whether the collection of certain information and the subsequent usage are fair relative to the context of the exchange.

Exchange fairness and cost-benefit tradeoff analysis are *separate but related* factors influencing the disclosure of personal information. Low fairness may cause consumers to withhold personal information even if benefits override the contemporary privacy costs. For example, demographic information like gender and age typically is considered to have low sensitivity and therefore, regarded as having a low disclosure risk. However, the collection of such information in a context that is irrelevant to the transaction may cause consumers to perceive the information exchange as unfair and raise an alert about potential privacy risk in the future. This may negatively influence willingness to disclose personal information. This is especially true for e-commerce transactions with unfamiliar websites, where consumers may simultaneously perceive high benefits and high costs due to the great uncertainty in the exchange. In general, perceptions of low fairness signals potential exchange risks [8].

Online firms could implement FIP principles to enhance perceived fairness and alleviate the effect of privacy costs on consumers' information disclosure intention [7, 8]. Internet users are generally concerned about the amount of information collected by an online vendor [27]. Collected information should be commensurate with the exchange benefits, implying that the nature of information requested should be *relevant* to the purpose of the transaction. This is consistent with FIP principles stated in OECD [34] about the purpose of the data collected, i.e. "only certain categories of data ought to be collected and, possibly, that data collection should be restricted to the minimum necessary to fulfill the specified purpose". Therefore, in this study, perceived fairness of information exchange is operationalized as perceived relevance of information, which is "the degree to which the data requested appear relevant or appear to have a bearing upon the purpose of the inquiry" [43]. A website collecting information relevant to the transaction would be deemed more likely to respect and protect information privacy. Conversely,

a website requesting irrelevant information would be considered more likely to violate information privacy through surreptitious use of the information for unauthorized purposes. Therefore,

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

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

Besides the effect on privacy perceptions, perceived 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. Therefore, we hypothesize:

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

Control variables

Six personal difference factors were also 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 control variables, 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 [39, 42] and was often found to exert weak influence or no influence over information disclosure in the existence of other predictor such as trust belief and risk belief [1, 27, 48]. In the presence of multiple situational factors at a specific level in our research model, the direct effect of privacy concern on behavioral intention is

expected to be unstable. Even a finding of a weak direct relationship will have limited external validity. So, privacy concern is included as a control variable.

RESEARCH METHODOLOGY

Study design and procedures

An experimental Web site that mimics a real commercial Web site providing Internet fax service was created for the purposes of this study. Monetary rewards were manipulated at two levels: no reward and reward ($10 off the service fee for two months). 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 potential customer searching for Internet 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, a security question used to validate identity (father's middle name, mother's maiden name, etc), and date of birth. As the last step of this study, subjects were required to fill out the survey measuring research constructs

Variable measurement

Existing published scales were adapted to measure variables in the research model. The perceived usefulness scale was adapted from the scale by Davis [9]. Perceived relevance items were modified from Stone [43]. Privacy protection belief was measured using the scales by Pavlou and Chellappa [35]. Privacy risk belief and behavioral intention were adapted from the

instruments by Malhotra et al [27]. Privacy concern consisted of three items developed by Malhotra et al [27] for measuring global information privacy concern. All constructs are measured on a seven-point Likert scales with 1 being “strongly disagree” and 7 being “strongly agree”. In addition, a single question (whether the website provided discounts or coupons for signing up with its service) was developed to check the manipulation on monetary rewards.

Survey administration

Before the final experiment, a pilot study was administered to 75 undergraduate and graduate students in a major Midwestern U.S. university 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		Internet Experience	
Male	66.5%	19-25 yr	94.5%	<1 yr	11.6%
Female	33.5%	26-30 yr	3.8%	1-3 yr	39.8%
		31-35 yr	1.1%	3-6 yr	33.1%
		>35 yr	0.5%	>=6 yr	15.5%

While some might be concerned about the use of student subjects, we do *not* believe that this concern seriously limits the generalizability of the results. Opponents of the use of student subjects claim that students are inappropriate surrogates for the “real world” when they are asked to imagine themselves in an organizational context. However, in this study, students are naturally a part of the population of interest as they have experiences in online shopping. In fact, according to the Pew Internet & American Life Project [36], the sample chosen is quite representative of

active Internet users (i.e., those between the ages of 19 and 25), making the sample highly appropriate for this context. Multiple prior studies on Internet-related behaviors and beliefs [e.g., 22, 26, 29] have used student samples positing that online consumers and Internet users are generally younger and more highly educated, thus making student samples closer to the online consumer population. Moreover, Nadkarni and Gupta indicated that there are no differences reported in student vs. non-student samples regarding studies of online behavior [33]. Therefore, along with some of the prior studies [e.g., 15, 23], we believe that student subjects are generally considered as a reasonable surrogate for online consumers.

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 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.

Measurement model

Results of testing the measurement model are presented in Tables 2 and 3. A scale is considered as reliable if its composite reliability (CR) is above 0.7 and average variance extracted (AVE) above 0.5 [2]. 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 constructs and all loadings except PPB5 are above 0.6, the recommended cutoff by Bagozzi and Yi [2]. But, the loading of PPB5 is still above 0.5, which is acceptable according to Chin [5]. Discriminant validity of each latent construct was tested by the method recommended by Fornell and Larcker [14]. 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.

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

		Loadings					
Constructs/Items		PU	PPB	PRB	RELE	BI	PC
Perceived Usefulness (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
Privacy Protection Belief	PPB1	0.273	**0.755**	-0.389	0.255	0.472	-0.158
(PPB)	PPB2	0.261	**0.779**	-0.409	0.376	0.453	-0.096
CR = 0.848	PPB3	0.206	**0.801**	-0.427	0.309	0.373	-0.113
AVE = 0.533	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
Privacy Risk Belief (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
Perceived Relevance (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
Behavioral Intention (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
Privacy Concern (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**

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.

Hypotheses testing results

Figure 2 summarizes the results of testing the hypotheses. Completely standardized path coefficients are given on each significant path. The model could explain 50.8% of the variance in behavioral intention.

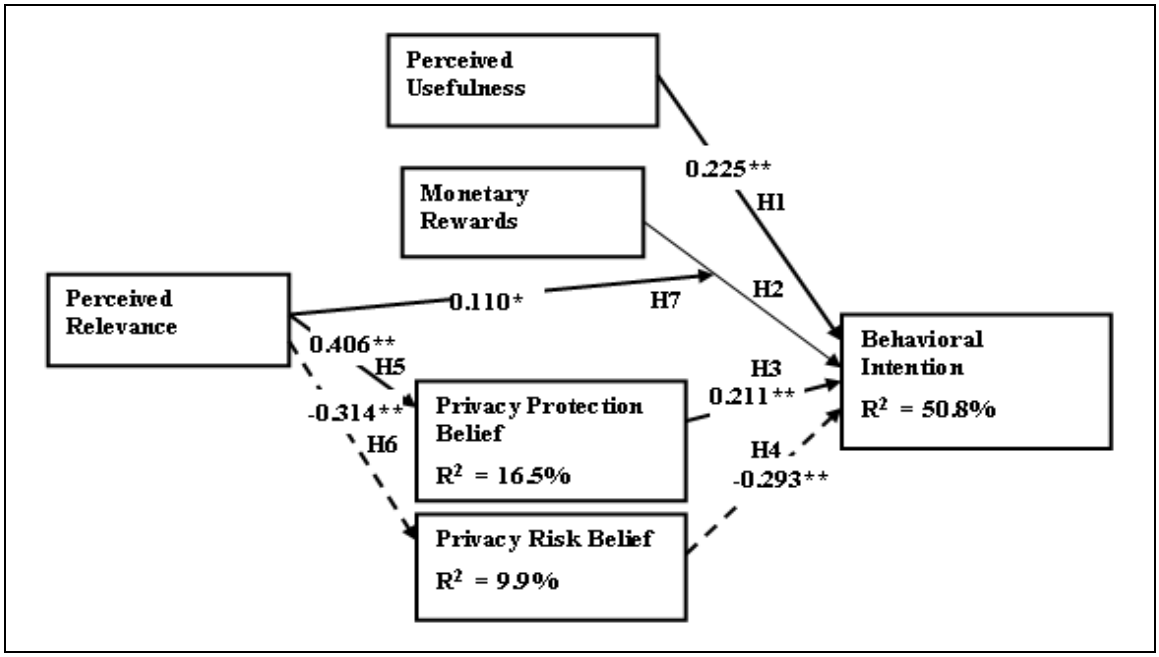

Figure 2: Results of testing hypotheses using PLS analysis. Completely standardized estimates, controlled for covariates in the research model, *p < 0.05, **p < 0.01.

We first analyzed the interaction effect or Hypothesis 7. 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 [6]. 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 shown 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. [38] 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. 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.

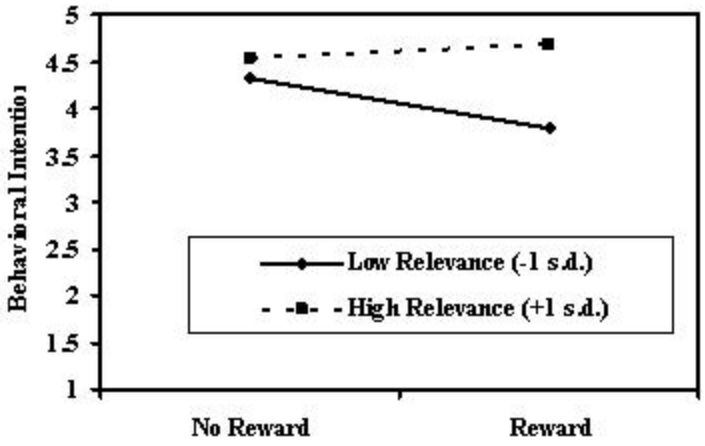

Figure 3: The moderation effect of perceived relevance on the relationship between monetary rewards and behavioral intention to disclose personal information.

Because the interaction is significant, main effect Hypothesis 2 cannot be interpreted. All other hypotheses were found to be statistically significant. Therefore, the overall research model

is well supported except for the unexpected interaction pattern. In addition, none of the six control variables were found to be significant.

DISCUSSIONS

Summary of findings and limitations

Our findings suggest that online shoppers' willing to disclose personal information is driven by exchange benefits, and 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 costs is further significantly influenced by the perceived fairness of information exchange. Collecting information of high relevance was found to enhance privacy protection belief and reduce privacy risk belief.

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 personal information. The undermining effect of rewards can be explained using cognitive evaluation theory, which states that such undermining could occur "when events are perceived to be influenced and controlled by extrinsic factors" (such as monetary rewards) [46, Page 364]. In the context of conventional marketplace or typical e-commerce transactions, monetary rewards are considered by consumers as benefits of the primary exchange. This represents the *normal* view of online shoppers or part of the social contract involved in information exchange. Online firms are likely to be viewed unfavorably when perceived as attempting to use monetary rewards to entice customers into information disclosure (or membership sign-up), or when online shoppers perceive a salient contingency between monetary rewards and information disclosure.

The fairness of information exchange is an important part of the social contract in information disclosure. Collecting irrelevant information is very likely to enhance the salience of the monetary reward's disclosure-contingency and the subsequent undermining effect.

Despite the overall support of the proposed model, this study has some potential limitations. First, although the student subjects in this study are reasonable surrogates for online shoppers, future research using a more diverse sample could help to further increase the generalizability of this research to the general population. Second, as the phenomenon of information privacy may be culturally dependent [31], the current research framework can be expanded to a cross-cultural context. To effectively build the information exchange relationships with consumers in each local market, it is essential that global marketers tailor for each country a proper practice of information collection and utilization. Prior privacy literature contains a few pioneering attempts at showing that the degree of privacy risk perceptions differs across countries [3, 10, 31, 32]. Future research could be designed to explore how consumers vary in their reactions to the privacy calculus in different cultures.

Contributions

The paper's primary contribution is integrating the concept of privacy calculus and social contract theory to empirically examine information exchange with unfamiliar Web sites. Such integration enhances our understanding about the complex process of privacy decisions/behaviors in a specific e-commerce transaction context involving primary exchange and second exchange with an unfamiliar Web site. Second, the study contributes to the privacy calculus perspective by viewing typical e-commerce transactions in the context of conventional ecommerce marketplace where the information exchange acts as a by-product of a primary exchange for products or services. Such a viewpoint is valuable in identifying motivators that

drive information disclosure considering the tight coupling between the primary exchange and the second information exchange. Attempting to understand privacy decisions/behaviors involved in information exchange without considering the motivators of the primary exchange is likely to result in potentially misleading theory and empirical results. For example, the benefits of the primary exchange and their potential interaction with cost/benefits factors of information exchange should not be ignored. Third, by considering the characteristics of a conventional marketplace, this study sheds light on identifying the shared implicit norms in the social contract governing information exchange. For example, in the conventional e-commerce marketplace, one of the shared understandings about monetary rewards is that they are usually offered as a way to attract online shoppers to complete the exchange for products or services, and not for luring consumers to disclose their personal information. Violation of such normal view is likely to result in the breaching of the social contract, and produce a negative impact of monetary rewards on information disclosure. Fourth, this study contributes to the online privacy literature by empirically validating the essential role of the exchange fairness in a privacy calculus behavior. Finally, from a descriptive perspective, the study illustrates that information disclosure in our context is a result of joint assessments about exchange costs, benefits and fairness.

Implications for research

The results of this study have five important implications for research. First, situational factors at a specific level are important drivers of online shoppers' willingness to disclose personal information, which tend to override the effect of inherent personal characteristics. This study provides empirical evidence for it. None of the personal difference variables was found to be significant determinant of information disclosure while all situational factors at a specific level are found to be significant determinants. This study examined a subset of the situational

factors at a specific level. Future studies could examine other situational factors at a specific level such as the design of the website.

Second, our findings show that benefits from the primary exchange such as perceived usefulness could also influence information disclosure. 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 for products or services and examine the impact of the benefits of the primary exchange on information disclosure as well.

Third, our results suggest that the effects of some primary-exchange benefits are dependent on the specific business context. 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, and reputation of the vendor. Future studies are needed to have a 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. 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? The results may be dependent upon individuals' preference of different type of benefits, types of products, or other factors associated with specific business context.

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. The theory accounts for not only the cost-benefit tradeoff among competing factors but also the adjustment by fairness of information disclosure. This is especially important for information disclosure in an online environment, which is considered as more uncertain than offline environments. Social contract theory recognizes the importance of such uncertainty in exchange and emphasizes that the cost-benefit tradeoff analysis of information disclosure should be subject to the assessment about the fairness of information exchange.

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 be aware that the benefits offered for the primary exchange may influence information disclosure as well. First of all, online vendors need to ensure the attractiveness of their products or services to the targeted customers such as usefulness of products. But, online vendors should be careful about providing monetary rewards to attract new customers. We found that, in a conventional e-commerce marketplace, monetary reward may have an adverse effect on consumers' willingness to disclose their personal information if the information collected is perceived to have no or low

relevance with the purpose of the ecommerce transaction. They should exercise care to ensure that only relevant information is collected.

In addition, 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.

Online vendors also need to take into account the fairness of information exchange. Online firms could implement fair information practices to boost fairness perceptions, 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 information disclosure intention.

CONCLUSIONS

Information privacy has become one of the primary factors that hinder the growth of e-commerce. The importance of privacy has attracted growing attention not only from managers but also from researchers in multiple disciplines such as marketing, law, management information systems, etc. 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

[1] 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, 13-28.

[2] Bagozzi, R. P. and Yi, Y., "On the evaluation of structural equation models," *Journal of the Academy of Marketing Science*, 16(1), 1988, 74-94.

[3] Bellman, S., Johnson, E. J., Kobrin, S. J., and Lohse, G. L., "International differences in information privacy concerns: A global survey of consumers," *Information Society*, 20(5), 2004, 313-324.

[4] Bennett, C. J., "Regulating Privacy: data protection and public policy in Europe and the United States," *Cornell University Press*, 1992,

[5] Chin, W. W., *The Partial Least Squares Approach for Structural Equation Modeling*, Lawrence Erlbaum, Mahway, New Jersey, 1998.

[6] Cohen, J., *Statistical power analysis for the behavior sciences*, Lawrence Erlbaum, Hillsdale, NJ, 1988,

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

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

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

[10] Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C., "Privacy Calculus Model in E-commerce - a Study of Italy and the United States," *European Journal of Information Systems*, 15(4), 2006, 389-402.

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

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

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

[14] Fornell, C. and Larcker, D., "Evaluating structural equation models with unobservable variables and measurement error," *Journal of Marketing Research*, 18(1), 1981, 39-50.

[15] Gefen, D., Karahanna, E., and Straub, D., "Trust and TAM in online shopping: an integrated model," *MIS Quarterly*, 27(1), 2003, 51-90.

[16] Gefen, D., Warkentin, M., Pavlou, P., and Rose, G., "EGoverment adoption," AMCIS 2002, 2002, 83

[17] Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., and Png, I. P. L., "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach," *Journal of Management Information Systems*, 24(2), 2007, 13-42.

[18] 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, 1-10

[19] 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, 129-139.

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

[21] Hui, K. L., Teo, H. H., and Lee, S. Y. T., "The value of privacy assurance: An exploratory field experiment," *MIS Quarterly*, 31(1), 2007, 19-33.

[22] Jiang, Z. and Benbasat, I., "Research note investigating the influence of the functional mechanisms of online product presentations," *Information Systems Research*, 18(4), 2007, 454-470.
[23] Kim, D. J., Ferrin, D. L., and Rao, H. R., "A trust-based consumer decision model in electronic commerce: The role of trust, perceived risk, and their antecedents," *Decision Support Systems*, 44(2), 2008, 544-564.
[24] Laudon, K. C., "Markets and privacy," *Communications of the ACM*, 39(9), 1996, 92-104.
[25] 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, 22-42.
[26] Limayem, M., Hirt, S. G., and Cheung, C. M. K., "How habit limits the predictive power of intention: The case of information systems continuance," *MIS Quarterly*, 31(4), 2008, 705-737.
[27] 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, 336-355.
[28] Margulis, S. T., "On the status and contribution of Westin's and Altman's theories of privacy," *Journal of Social Issues*, 59(2), 2003, 411-429.
[29] McKnight, D. H., Choudhury, V., and Kacmar, C., "Developing and validating trust measures for e-commerce: an integrative typology," *Information Systems Research*, 13(3), 2002, 334-359.
[30] Metzger, M. J., "Privacy, trust, and disclosure: exploring barriers to electronic commerce," *Journal of Computer-Mediated Communication*, 9(4), 2004,
[31] Milberg, S. J., Smith, H. J., and Burke, S. J., "Information privacy: Corporate management and national regulation," *Organization Science*, 11(1), 2000, 35-57.
[32] Milberg, S. J. B., J.S., Smith, H. J., and Kallman, A. E., "Values, Personal Information Privacy Concerns, and Regulatory Approaches," *Communication of the ACM*, 38(12), 1995, 65-74.
[33] Nadkarni, S. and Gupta, R., "A task-based model of perceived website complexity," *MIS Quarterly*, 31(3), 2008, 501-524.
[34] Organization for Economic Cooperation and Development, *Guidelines on the protection of privacy and transborder flows of personal data*, 1980.
[35] 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., 2001.
[36] PEW-Internet, *Pew Internet & American Life Project: Demographics of Internet Users*, 2008.
[37] Phelps, J., Nowak, G., and Ferrell, E., "Privacy concerns and consumer willingness to provide personal information," *Journal of Public Policy Marketing*, 19(1), 2000, 27-41.
[38] 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.
[39] Smith, H. J., Milberg, S. J., and Burke, S. J., " Information Privacy measuring individuals' concerns about organizational practices," *MIS Quarterly*, 20(2), 1996, 167-196.
[40] Solove, D. J., "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, 154(3), 2006, 477-560.
[41] Son, J.-Y. and Kim, S. S., "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly*, 32(3), 2008, 503-529.
[42] Stewart, K. A. and Segars, A. H., "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research*, 13(1), 2002, 36-49.
[43] 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.
[44] 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, 459-468.
[45] Teltzrow, M. and Kobsa, A., *Impacts of user privacy preferences on personalized systems: A comparative study.* , Kluwer Academic Publishers, Dordrecht, Netherland, 2004.
[46] Tietje, B. C., "When do rewards have enhancement effects? An availability valence approach," *Journal of Consumer Psychology*, 12(4), 2002, 363-373.
[47] USC, *Online World As Important to Internet Users as Real World?*, Center for the Digital Future, Annenberg School for Communication, University of Southern California, 2007.
[48] Van Slyke, C., Shim, J. T., Johnson, R., and Jiang, J., "Concern for information privacy and online consumer purchasing," *Journal of the Association for Information Systems*, 7(6), 2006, 415-444.

[49] Wang, Y.-S., Wang, Y.-M., Lin, H.-H., and Tang, T.-I., "Determinants of user acceptance of Internet banking: an empirical study," *Journal: International Journal of Service Industry Management*, 14(5), 2003, 501-519.

[50] Westin, A. F., *Privacy and Freedom*, Atheneum, New York, 1967,

[51] Xu, H., Dinev, T., Smith, H. J., and Hart, P., "Examining the formation of individual's privacy concerns: Toward an integrative view," Proceedings of 29th Annual International Conference on Information Systems (ICIS 2008), Paris, France, 2008,