

December 2003

# Consumer Trust and Online Information Privacy

Yunjie Xu

*National University of Singapore*

Bernard Tan

*National University of Singapore*

Kai-Lung Hui

*National University of Singapore*

Follow this and additional works at: <http://aisel.aisnet.org/icis2003>

---

## Recommended Citation

Xu, Yunjie; Tan, Bernard; and Hui, Kai-Lung, "Consumer Trust and Online Information Privacy" (2003). *ICIS 2003 Proceedings*. 45.  
<http://aisel.aisnet.org/icis2003/45>

This material is brought to you by the International Conference on Information Systems (ICIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ICIS 2003 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact [elibrary@aisnet.org](mailto:elibrary@aisnet.org).

# CONSUMER TRUST AND ONLINE INFORMATION PRIVACY

**Yunjie Xu, Bernard C. Y. Tan,  
Kai-Lung Hui, and Wai-Kiat Tang**  
Department of Information Systems  
National University of Singapore  
Singapore

[xuyj@comp.nus.edu.sg](mailto:xuyj@comp.nus.edu.sg)      [btan@comp.nus.edu.sg](mailto:btan@comp.nus.edu.sg)  
[lung@comp.nus.edu.sg](mailto:lung@comp.nus.edu.sg)      [tangwaik@comp.nus.edu.sg](mailto:tangwaik@comp.nus.edu.sg)

## Abstract

*Getting consumers to disclose their personal information is an essential first step for Internet businesses that choose to pursue a niche marketing strategy. Previous research has examined how the reward preferences and privacy concerns of consumers may affect their disclosure tendency. However, it is not known how key characteristics pertaining to Internet businesses, such as consumer trust, may affect disclosure tendency. Based on the results obtained from a survey, this study found that consumer trust in Internet businesses can facilitate disclosure tendency. Moreover, consumer trust can suppress the reward preferences and privacy concerns of consumers, thereby reducing the costs that Internet businesses need to incur in collecting personal information from consumers.*

**Keywords:** Information privacy, information disclosure, reward preference, privacy concern, consumer trust

## Introduction

An important benefit that electronic commerce promises is the opportunity for mass customization. With sufficient consumer information, Internet businesses can cater to the specific needs of consumers in a timely fashion. Whether such a promise can be fulfilled or not depends on the ability of Internet businesses to collect personal information from consumers. Hoffman et al. (1999) report that “almost 95% of consumers have declined to provide personal information to websites and 63% of these indicated this is because they do not trust those collecting the data.” Lack of consumer trust for Internet businesses seems to be a critical barrier that hinders the efforts of Internet businesses to collect personal information from consumers for the purpose of mass customization.

Prior research has suggested that the tendency of consumers to disclose personal information online can be affected by their privacy concerns and reward preferences. Privacy concern is a multidimensional construct: consumers are concerned about the collection of, unauthorized secondary use of, improper access to, and errors in storing their personal information by Internet businesses (Culnan 1993; Smith et al. 1996; Stewart and Segars 2002). Measures such as fair information practices and confidentiality assurance to consumers may ease privacy concerns and encourage disclosure of personal information (e.g., Culnan and Armstrong 1999; Milberg et al. 2000). Providing the right rewards can also induce consumers to disclose personal information online (Hann et al. 2002; Tam et al. 2002). The rewards preferred by consumers may be extrinsic (e.g., monetary savings and time savings) or intrinsic (e.g., pleasure and altruism) in nature (Tam et al. 2002). In practice, Internet businesses may simultaneously attempt to alleviate the privacy concerns and meet the reward preferences of consumers so as to induce consumers to disclose their personal information.

Measures to meet reward preferences or alleviate privacy concerns of consumers do not come free. For example, Hann et al. (2002) estimate that the costs to remove the privacy concerns of all U.S. Internet and e-mail users may range from US \$4.56 billion to US \$5.70 billion in 2001. The actual costs incurred by Internet businesses may be contingent upon some key

characteristics, one of which is consumer trust. Internet businesses that are considered trustworthy by consumers may incur lower costs in meeting reward preferences because consumers tend to require less reward for motivating them to provide personal information to such businesses. Internet businesses that are considered trustworthy by consumers may also incur lower costs in alleviating privacy concerns because consumers tend to have less privacy concerns when providing personal information to such businesses. In short, consumer trust may moderate the impact of reward preferences or privacy concerns on disclosure tendency. To date, the role of consumer trust in the context of online information disclosure is not well investigated by researchers.

Focusing on the issue of consumer trust, this study seeks answers to two research questions: (1) How does consumer trust affect consumer tendency to disclose personal information to Internet businesses? (2) How does consumer trust moderate the impact of reward preferences or privacy concerns on such disclosure tendency? From a theoretical perspective, this study adds the important element of consumer trust to recent efforts to build a theory explaining the disclosure tendency by consumers of Internet businesses. From a practical perspective, the results of this study can offer Internet businesses some suggestions on how they could induce their consumers to disclose personal information under varying conditions of consumer trust.

## Conceptual Background and Hypotheses

The social exchange theory posits that reward and cost factors determine the development of social relationships (Thibaut and Kelly 1959). The rewards are positive returns from exhibiting certain behavior within these relationships. The costs are factors that inhibit or deter the performance of a sequence of behavior that sustains the relationship. The relationship between consumers and Internet businesses can be viewed as a type of such social relationships (Tam et al. 2002). When Internet businesses meet the reward preferences of consumers, consumers should exhibit the behavior of disclosing personal information. However, privacy concerns represent cost factors that can potentially inhibit consumers from disclosing personal information, thereby disrupting the relationship. Based on the social exchange theory, attempts by Internet businesses to meet reward preferences (supplying reward) and alleviate privacy concerns (reducing cost) should encourage online information disclosure by consumers.

Rewards given to consumers may be extrinsic or intrinsic in nature (Tam et al. 2002). Extrinsic rewards that have been found to be useful to induce information disclosure include monetary savings (e.g., give discount coupons in exchange for personal information), time savings (e.g., provide customized Websites in exchange for personal information), self-concept enhancement (e.g., allow consumers to become members of exclusive virtual clubs when they provide personal information), and social adjustment (e.g., give consumers the means to conform to the norms of valued reference groups when they provide personal information) (Tam et al. 2002). Intrinsic rewards that have been reported to be useful to induce information disclosure include pleasure (e.g., provide consumers with an enjoyable experience in exchange for personal information), novelty (e.g., give consumers opportunities to explore issues that they value when they provide personal information), and altruism (e.g., appeal to the desire of consumers to help others when getting their personal information) (Tam et al. 2002). Different consumers have different reward preferences. If a consumer has a stronger preference for a certain type of reward, in order to enjoy it when it is present, the consumer will be more willing to disclose personal information. Hence, the extent to which providing each type of reward can induce information disclosure would depend on the preference of a consumer for that particular type of reward.

*H1a: Consumers will be more willing to disclose personal information if Internet businesses meet their specific reward preferences.*

Privacy concerns that have been reported to inhibit information disclosure by consumers include inappropriate collection of personal information (e.g., collect too much consumer information), unauthorized secondary use of personal information (e.g., use consumer information for spam or promotion), improper access to personal information (e.g., transfer consumer information to other business units), and errors in storing personal information (e.g., use outdated consumer information) (Smith et al. 1996; Stewart and Segars 2002). Different consumers may have different privacy concerns. For instance, if a consumer is concerned about improper access, then she will be more willing to disclose personal information when a Website takes precautionary measures to ensure that her information is not accessible by unauthorized persons. Thus, the extent to which alleviating each type of concern can induce information disclosure would depend on whether a consumer has that particular concern.

*H1b: Consumers will be more willing to disclose personal information if Internet businesses alleviate their specific privacy concerns.*

Besides reward preferences and privacy concerns, consumers are also affected by their trust for Internet businesses when deciding whether or not to disclose personal information (Culnan and Bies 2003). Consumer trust induces disclosure tendency because it lowers the risk perception of consumers. An objective evaluation of risk (e.g., probability of information misuse) is typically infeasible because the consumer may not have adequate information about, or prior experience with, the Internet businesses that solicit their personal information. Yet, before they know enough about these Internet businesses, consumers often have to decide whether or not to give personal information to these Internet businesses for carrying out transactions (e.g., purchase products or services, and sign up as members of virtual clubs). This “willingness to be vulnerable” in taking a risky action, on the part of consumers, reflects consumer trust (Mayer et al. 1995). Sometimes, such consumer trust is formed based on limited information about, or prior experience with, the Internet business. By lowering their risk perception (Javenpaa et al. 2000; Mayer et al. 1995; McKnight et al. 2002), such consumer trust causes a “leap in faith” which results in risk-taking behavior by consumers (Lewis and Weigert 1985).

An extensive body of research has reported that trust is a direct cause of cooperative behavior (Dirks and Ferrin 2001). In the context of Internet businesses, consumer trust alone may induce consumers to disclose their personal information, irrespective of whether there are efforts to meet reward preferences or alleviate privacy concerns. Trustworthiness, in the form of competence, benevolence, and integrity of businesses, has been reported to bring about online information disclosure (Mayer et al. 1995). Consumers may be more willing to disclose personal information to Internet businesses that are perceived to be competent in providing basic services, helpful in handling consumer requests, and honest in handling transactions. Therefore, consumer trust is likely to have a direct impact on disclosure tendency.

*H2: Consumers will be more willing to disclose personal information if Internet businesses have their trust.*

Besides directly affecting disclosure tendency, consumer trust may also moderate the impact of reward preferences and privacy concerns on disclosure tendency. In business transactions, people tend to observe risk-return tradeoffs, and demand less rewards if the probability of getting the rewards is higher (Tversky et al. 1988). Following this line of argument, consumers may demand less rewards from trusted Internet businesses in exchange for their personal information because the probability of getting the rewards from trusted Internet businesses should be higher. Hence, rewards preferences can be suppressed in the presence of consumer trust. That is, the *more* a consumer trusts a company, the *less* the consumer cares about rewards. If the company is not trusted by the consumer, then it may need to give more rewards to induce the consumer to disclose personal information.

*H3a: The relationship between meeting specific reward preferences and the disclosure of personal information will be stronger under conditions of low consumer trust than high consumer trust.*

Schur and Ozanne (1985) observe that, in a trustor-trustee relationship, the trustor tends to have less desire to bargain and is usually more willing to accommodate the trustee if the trustee is reliable. By the same token, consumer trust can alter the significance of privacy concerns to consumers. Consumers may be more willing to accommodate the requests of Internet businesses that solicit personal information if these businesses are considered trustworthy. Consumers may have less of a desire to demand privacy protection mechanisms, given the presence of consumer trust. Hence, privacy concerns can be suppressed in the presence of consumer trust. In other words, the *more* the consumer trusts the business, the *less* the consumer cares about the privacy protection mechanisms. On the contrary, for a less-trusted company, a consumer may expect strong privacy protection.

*H3b: The relationship between alleviating specific privacy concerns and disclosure of personal information will be stronger under conditions of low consumer trust than high consumer trust.*

## Methodology

The survey research method was used for data collection. Scales were developed to measure the seven types of reward preferences, the four types of privacy concerns, consumer trust, and disclosure tendency. These scales were then consolidated into a questionnaire and administered to subjects.

### Scale Development

Questions to measure the seven types of reward preferences were adapted from an instrument presented in Tam et al. (2002). This instrument had a total of 26 questions to assess the preferences for monetary savings, time savings, self-concept enhancement, social adjustment, pleasure, novelty, and altruism. All questions were anchored on seven-point Likert scales.

Questions to measure the four types of privacy concerns were adapted from an instrument developed and validated by Smith et al. (1996). This instrument had a total of 15 questions to assess the four dimensions of privacy concerns: excessive collection of, unauthorized secondary use of, improper access to, and errors in storing personal information. To assess the effects of alleviating privacy concerns, these questions were reworded as questions measuring consumer preference for privacy protections. For example, regarding the error in stored information, an original question asking about consumer concern on storing erroneous information was reworded as a question asking about consumer preference for procedures to correct erroneous information. Such revision is grounded on Fair Information Practices, which require data collectors to offer mechanisms to maintain the accuracy of the collected information. The reworded questions were also similar in nature to those measuring reward preferences. All questions were anchored on seven-point Likert scales.

Eight questions to measure consumer trust were modified from an instrument presented in Doney and Cannon (1997). All questions were anchored on seven-point Likert scales. To increase the generalizability of the result, three different scenarios of online information solicitation were created. In the three scenarios, the three Internet businesses soliciting consumer information were *Nokia Club* (see [www.club.nokia.com.sg](http://www.club.nokia.com.sg)), *Iguana Mobile* (see [www.apic.com.sg](http://www.apic.com.sg)), and *MiReDo Tones* (a fictitious company). These companies represent different scales of operations in the same industry.

To assess disclosure tendency (the dependent variable), self-generated questions were used to measure consumer intention to provide personal information to Internet businesses. A baseline question assessed disclosure intention in the absence of any effort to meet reward preferences or alleviate privacy concerns. Seven other questions assessed disclosure intention in the presence of each of the seven types of rewards (which corresponded to efforts to meet the seven reward preferences). Four other questions assessed disclosure intention in the presence of each of the four types of privacy protections (which corresponded to efforts to alleviate each of the four types of privacy concerns). All questions were anchored on seven-point Likert scales. The difference in disclosure intention between each of the seven questions (with rewards) and the baseline question reflected the impact of providing each type of reward. The difference in disclosure intention between each of the four questions (with privacy protections) and the baseline question reflected the impact of alleviating each type of privacy concern. Using such differences in disclosure intention as the dependent variable also had the advantage of cancelling out spurious (e.g., individual-specific) factors affecting disclosure tendency.

**Data Collection**

The survey was administered to 360 senior undergraduate students enrolled in an electronic commerce course. A major assignment in this course was to develop a functional retail Website. Thus, all the subjects who participated in this study should have been familiar with both technical and managerial issues pertaining to Internet businesses. Given that consumers of Internet businesses are generally younger and highly educated, this sample of subjects should be reasonably representative of such consumers. Table 1 gives the general statistics of the subjects.

The purpose of the research was not disclosed to the subjects before the survey. The three scenarios (*Nokia Club*, *Iguana Mobile*, and *MiReDo Tones*) were randomly assigned to the subjects. Although all of the subjects voluntarily participated in this study, those who completed the survey were given a token payment. Altogether, 331 usable responses were collected, with 112 responses for *Nokia Club*, 110 responses for *Iguana Mobile*, and 109 responses for *MiReDo Tones*.

**Table 1. Subject Background**

Statistics	Average	Standard deviation
Age	22.0	1.4
Internet usage (hours/week)	34.7	27.8
Online disclosure experience (number of Websites in the last 12 months)	7	9.5
Online purchase experience (percent)	41.2%	n/a

## Analyses and Results

All statistical tests were carried out at a 5 percent level of significance.

### Measurement Model

The measurement properties of all the questions that measured reward preferences, privacy concerns, and consumer trust were assessed. Cronbach’s alpha, composite reliability, and average variance extracted were computed for each construct to check for reliability (see Table 2). A construct had adequate reliability if the Cronbach’s alpha was at least 0.7, composite reliability was at least 0.7, and average variance extracted was at least 0.5 (Bagozzi and Yi 1988; Nunnally 1978). Separate confirmatory factor analyses (using LISREL 8.51) were conducted to examine the convergent and discriminant validity of each set of questions (see Table 2). For brevity, standardized factor loadings for all questions (on their intended constructs) were not reported.

All seven constructs reflecting reward preferences had adequate reliability (see Table 2). The goodness-of-fit index (GFI) for the measurement model (7 constructs, 26 questions) was 0.86, a marginally acceptable level (Hu and Bentler 1995). Both the root mean square residuals (RMR) and the root mean square error of approximation (RMSEA) for this measurement model were 0.067, which was within the acceptable range (Hair et al. 1995) (see Table 3). Standardized factor loadings for all (but one) questions were greater than the recommended threshold of 0.50 (Hair et al. 1995). One question for social adjustment had a factor loading of 0.46, which was close to the recommended threshold. The t-statistics of all factor loadings were substantial and significant ( $p < 0.01$ ). Overall, this measurement model was adequate.

All four constructs reflecting privacy concerns also had adequate reliability (see Table 2). The goodness-of-fit index (GFI) for the measurement model (4 constructs, 15 questions) was 0.92, an acceptable level. The root mean square residuals (RMR) and the root mean square error of approximation (RMSEA) for this measurement model were also within the acceptable range (see Table 3). Standardized factor loadings for all questions were greater than the recommended threshold of 0.50. The t-statistics of all factor loadings were substantial and significant ( $p < 0.01$ ). Overall, this measurement model was also adequate.

The consumer trust construct had adequate reliability (see Table 2). For this construct, two questions were dropped due to low standardized factor loadings (both below 0.40), leaving only six questions that measured the construct. After dropping the two questions, the goodness-of-fit index (GFI), root mean square residuals (RMR), and root mean square error of approximation (RMSEA) were within the acceptable range (see Table 3).

**Table 2. Reliability**

Construct	Composite Reliability	Cronbach’s Alpha	Average Variance Extracted
Monetary savings (MS)	0.91	0.91	0.72
Time savings (TS)	0.81	0.80	0.60
Self-concept enhancement (SC)	0.84	0.84	0.64
Social adjustment (SA)	0.75	0.73	0.50
Pleasure (PL)	0.86	0.85	0.67
Novelty (NV)	0.85	0.85	0.54
Altruism (AL)	0.91	0.91	0.66
Inappropriate collection (IC)	0.81	0.81	0.52
Unauthorized secondary use (US)	0.87	0.87	0.64
Improper access (IA)	0.85	0.85	0.65
Errors in storing (ES)	0.82	0.81	0.53
Consumer trust (CT)	0.87	0.86	0.54

**Table 3. LISREL Fit Indices**

Index	Reward Preferences (7 Constructs, 26 Questions)	Privacy Concerns (4 Constructs, 15 Questions)	Consumer Trust (1 Construct, 6 Questions)
Chi-square (df)	690.42 (278)	228.53 (84)	50.96 (9)
GFI	0.86	0.92	0.95
AGFI	0.83	0.88	0.89
RMR	0.067	0.043	0.041
RMSEA	0.067	0.072	0.120

**Hypotheses Testing**

After ensuring that the measurement properties of all questions had adequate reliability and validity, the measure for each construct was computed by averaging all of its questions. During hypotheses testing, a separate multiple regression analysis was carried out for each reward preference and each privacy concern. Therefore, the hypotheses were tested using a set of 11 regression analyses (corresponding to the seven reward preferences and the four privacy concerns).

For each multiple regression equation, there were two independent variables, one for the level of reward preference or privacy concern (to test H1a and H1b) and the other for the level of consumer trust (to test H2), as well as an interaction term involving these two independent variables (to test H3a and H3b). The dependent variable was measured by the question that asked subjects for their disclosure intention (DI) when a specific reward preference was met, or when a specific privacy concern was alleviated. For example, the regression equation for monetary savings would be  $DI(MS) = MS + CT + MS \times CT$ .

The results of these multiple regression analyses revealed that there were significant collinearity problems. The variance inflation factors and condition indices greatly exceeded the acceptable values of 10 and 30 (Hair et al. 1995) respectively in all of the analyses. The collinearity problem led to estimation inefficiency and made it difficult to interpret the regression coefficients or draw meaningful conclusions. To overcome this problem, the hypothesis testing was carried out in two stages instead.

In the first stage, 11 multiple regression analyses were used to test H1a, H1b, and H2. As before, there were two independent variables, one for the level of reward preference or privacy concern (to test H1a and H1b) and the other for the level of consumer trust (to test H2). The interaction term was dropped because H3a and H3b were not being tested at this stage. The same dependent variable was used. Hence, the regression equation for monetary savings would be  $DI(MS) = MS + CT$ .

Table 4 shows the results of the 11 multiple regression analyses. The variance inflation factors (VIF) and condition indices (CI) were acceptable, indicating no collinearity problem. All the regression coefficients were positive and significant (see Table 4). H1a, H1b, and H2 were supported. If consumers had a specific reward preference, meeting that reward preference (by providing the corresponding reward) increased their tendency to disclose personal information. If consumers had a specific privacy concern, alleviating that privacy concern (by implementing the corresponding protection) increased their tendency to disclose personal information. Moreover, the presence of consumer trust also increased the tendency of consumers to disclose personal information to Internet businesses.

In the second stage, another 11 multiple regression analyses were performed to assess H3a and H3b. In these regressions, an independent variable for the level of reward preference or privacy concern and an interaction term involving the independent variable and consumer trust were used. The dependent variable was constructed by subtracting the baseline disclosure intention (BL; i.e., no reward preferences were met and no privacy concerns were alleviated) from the disclosure intention (DI) by the same subject when a specific reward preference was met or a specific privacy concern was alleviated. This subtraction helped eliminate individual-specific characteristics, including consumer trust, which might affect disclosure intention. Therefore, consumer trust need not be included as an independent variable in these analyses. This could help resolve the collinearity problem between consumer trust and the interaction term. In short, the regression equation for monetary savings would be  $DI(MS) - B = MS + MS \times T$ .

**Table 4. Results of First Stage Analyses**

Multiple Regression Equation	Predictors	Coefficient	Std. Error	p	R <sup>2</sup>	VIF	CI
DI(MS) = MS + CT	MS	0.32	0.05	0.01	0.09	1.00	13.54
	CT	0.38	0.08	0.01			
DI(TS) = TS + CT	TS	0.21	0.06	0.01	0.10	1.03	13.76
	CT	0.31	0.07	0.01			
DI(SC) = SC + CT	SC	0.18	0.06	0.01	0.10	1.06	12.48
	CT	0.30	0.07	0.01			
DI(SA) = SA + CT	SA	0.28	0.07	0.01	0.12	1.04	13.30
	CT	0.32	0.07	0.01			
DI(PL) = PL + CT	PL	0.25	0.06	0.01	0.13	1.02	13.39
	CT	0.37	0.07	0.01			
DI(NV) = NV + CT	NV	0.26	0.07	0.01	0.07	1.01	15.36
	CT	0.24	0.07	0.01			
DI(AL) = AL + CT	AL	0.16	0.07	0.03	0.04	1.03	13.08
	CT	0.19	0.08	0.02			
DI(IC) = IC + CT	IC	0.28	0.08	0.01	0.09	1.01	17.87
	CT	0.34	0.08	0.01			
DI(US) = US + CT	US	0.75	0.07	0.01	0.30	1.00	18.88
	CT	0.27	0.07	0.01			
DI(IA) = IA + CT	IA	0.75	0.07	0.01	0.27	1.00	18.53
	CT	0.30	0.08	0.01			
DI(ES) = ES + CT	ES	0.50	0.07	0.01	0.17	1.01	15.51
	CT	0.18	0.07	0.02			

Table 5 presents the results of the 11 multiple regression analyses. The variance inflation factors (VIF) and condition indices (CI) showed that there was no collinearity problem. All the regression coefficients for the independent variable (except for altruism) were positive and significant (see Table 5). These results reinforced the support for H1a and H1b presented earlier in Table 4. All coefficients of the interaction term were negative (see Table 5), supporting H3a and H3b. However, four of these coefficients (for monetary savings, social adjustment, pleasure, and inappropriate collection) were not significant. Therefore, the moderating impact of consumer trust appeared to be modest. Nevertheless, consumer trust seemed to suppress the relationship between reward preferences and disclosure intention (if the reward preferences were met), and the relationship between privacy concerns and disclosure intention (if the privacy concerns were alleviated). With consumer trust, Internet businesses could put in less effort to meet reward preferences or alleviate privacy concerns and still obtain personal information from their consumers.

## Discussion

The results of this study show that Internet businesses can obtain personal information from their consumers by trying to meet the reward preferences of these consumers. Providing such valued rewards to consumers is consistent with the benefit congruency principle of marketing (Chandon et al. 2000), and the compatibility principle of psychology (Tversky et al. 1988). Seven types of rewards that may be employed to enhance the effectiveness of online marketing are monetary savings, time savings, self-concept enhancement, social adjustment, pleasure, novelty, and altruism (Tam et al. 2002). These results also show that Internet businesses can obtain personal information from their consumers by trying to alleviate the privacy concerns of these consumers. Four types of protections that may be put in place are protections against inappropriate collection of, unauthorized secondary use of, improper access to, and errors in storing personal information (Smith et al. 1996).

**Table 5. Results of Second Stage Analyses**

Multiple Regression Equation	Predictors	Coefficient	Std. Error	p	R <sup>2</sup>	VIF	CI
DI(MS) – BL = MS + MS×CT	MS MS×CT	0.41 -0.03	0.12 0.02	0.01 0.13	0.05	2.45	14.63
DI(TS) – BL = TS + TS×CT	TS TS×CT	0.44 -0.04	0.10 0.02	0.01 0.01	0.05	2.25	16.15
DI(SC) – BL = SC + SC×CT	SC SC×CT	0.35 -0.05	0.13 0.02	0.01 0.03	0.02	2.86	15.24
DI(SA) – BL = SA + SA×CT	SA SA×CT	0.40 -0.04	0.13 0.02	0.01 0.08	0.03	2.31	15.62
DI(PL) – BL = PL + PL×CT	PL PL×CT	0.40 -0.03	0.12 0.02	0.01 0.15	0.04	2.34	15.18
DI(NV) – BL = NV + N×CT	NV N×CT	0.54 -0.06	0.13 0.02	0.01 0.01	0.05	1.81	16.56
DI(AL) – BL = AL + AL×T	AL AL×CT	0.20 -0.05	0.15 0.02	0.19 0.04	0.01	2.58	15.58
DI(IC) – BL = IC + IC×CT	IC IC×CT	0.64 -0.03	0.11 0.02	0.01 0.12	0.11	1.38	16.24
DI(US) – BL = US + US×T	US US×CT	1.04 -0.04	0.11 0.01	0.01 0.01	0.24	1.40	18.55
DI(IA) – BL = IA + IA×CT	IA IA×CT	0.99 -0.03	0.11 0.02	0.01 0.03	0.21	1.41	18.16
DI(ES) – BL = ES + ES×CT	ES ES×CT	0.76 -0.06	0.11 0.02	0.01 0.01	0.13	1.76	16.30

Consumer trust seems to affect disclosure tendency in two ways. First, consistent with prior studies (e.g., McKnight et al. 2002), consumer trust for Internet businesses seems to directly increase the willingness of consumers to provide personal information to these businesses, irrespective of whether efforts have been made to meet reward preferences or alleviate privacy concerns. Second, consumer trust seems to suppress reward preferences and privacy concerns of consumers, thereby reducing the need for Internet businesses to meet reward preferences or alleviate privacy concerns when attempting to solicit personal information from consumers. This may greatly reduce the costs or efforts to collect such information, which is needed for focused marketing efforts. Efforts by Internet businesses to build consumer trust are worthwhile because consumer trust is an organizational asset.

These results must be interpreted in the context of the limitations of this study. One clear limitation is the use of student subjects. Although these subjects are familiar with both technical and managerial issues pertaining to Internet businesses, they may have little prior experience carrying out transactions with (and providing personal information to) actual Internet businesses. Compared to actual consumers, the student subjects may have weaker reward preferences, privacy concerns, or consumer trust. This study needs to be replicated with a sample of actual consumers of Internet businesses. Another limitation is the collinearity problems encountered during hypotheses testing. Instead of testing all of the hypotheses together, a two-stage approach had to be used. More research work is needed to understand the collinearity problems between consumer trust and the interaction term. This study needs to be replicated across a variety of settings to assess the robustness of the results. However, in spite of these limitations, the results of this study offer important theoretical and practical implications.

***Theoretical Implications***

This study builds on the findings of prior research in several ways. First, it establishes the usefulness of the seven reward preferences (Tam et al. 2002) in motivating consumers to provide their personal information to Internet businesses. Second, earlier studies have identified four privacy concerns (Smith et al. 1996; Stewart and Segars 2002) that can inhibit information

disclosure. This study verifies the usefulness of privacy protections, for these four privacy concerns, in motivating consumers to provide their personal information to Internet businesses.

Third, this study introduces the factor of consumer trust into research about online information privacy. By directly impacting disclosure tendency, consumer trust may be considered a substitute for meeting reward preferences or alleviating privacy concerns when eliciting personal information. By suppressing consumer desire for rewards or privacy protections, consumer trust may be seen as a trade-off for meeting reward preferences or alleviating privacy concerns when eliciting personal information. More research work is clearly needed before the factor of consumer trust can be integrated into any theory in the area of online information privacy. Nevertheless, this study opens up a broader research issue. Considering that reward preferences and privacy concerns are personal factors and that consumer trust is an organizational factor (some Internet businesses are more trusted by a general body of consumers than others), the results of this study raise interesting research questions about how various personal factors may substitute or trade off with various organizational factors (e.g., brand reputation) in affecting disclosure tendency by consumers. Also, the trade-offs among personal factors (e.g., meeting a specific reward preference but not alleviating a specific privacy concern) can be examined for the impact on disclosure tendency under varying levels of consumer trust.

### ***Practical Implications***

Internet businesses can obtain personal information about their consumers by meeting their reward preferences. Some organizations have offered such rewards when their consumers provide personal information online (Tam et al. 2002). Examples of businesses that have offered monetary savings or time savings include AT&T, Sprint, and Dell. Businesses that have offered self-concept enhancement or social adjustment include Macromedia and ZD Net. Businesses that have provided rewards to consumers in the form of pleasure and novelty include CD Now and Disney. Businesses that have appealed to the altruism of consumers include Salvation Army and United Nations Children's Fund. To understand the reward preferences of their consumers, Internet businesses may administer the instrument used in this study to their customers.

Internet businesses can also elicit personal information of their consumers by alleviating their privacy concerns. Smith (1994) describes how seven organizations in four different industries have responded to privacy concerns of their consumers by putting together some privacy protection mechanisms to alleviate these concerns. Such mechanisms may help to raise the willingness of consumers to disclose their personal information (Culnan 1993). Again, to understand the privacy concerns (and desired privacy protections) of their consumers, Internet businesses may administer the instrument used in this study to their customers.

As Internet businesses attempt to meet reward preferences or alleviate privacy concerns (or do both) to elicit personal information from consumers, they must be cognizant of the role that consumer trust plays in this process. Different measures can be used for existing consumers and new consumers. When dealing with existing consumers (where consumer trust is likely to be high), consumer trust can be used to elicit personal information. Internet businesses may want to emphasize their past competence (e.g., how they have provided good basic services), benevolence (e.g., how they have been helpful in handling consumer requests), and integrity (e.g., how they have been honest in handling transactions) (Mayer et al. 1995). They can explain how acquiring additional personal information from consumers can help them do even better in terms of competence, benevolence, and integrity. This may motivate some existing consumers to disclose their personal information. In this case, it may be less costly for Internet businesses to rely on consumer trust (compared to meeting reward preferences or alleviating privacy concerns) to collect personal information.

When dealing with new consumers (where consumer trust is likely to be low), Internet businesses are likely to have to rely on meeting reward preferences or alleviating privacy concerns to collect personal information from consumers. Depending on the nature of their businesses, some types of rewards may be more salient (Tam et al. 2002) and some types of privacy protection mechanisms may be more feasible (Smith 1994). Internet businesses need to study new consumers carefully to understand their reward preferences and privacy concerns. Given that consumer trust is an organizational asset, Internet businesses should also undertake efforts to build consumer trust (McKnight et al. 2002). These efforts should focus on establishing perceived competence (e.g., provide good basic services), benevolence (e.g., be helpful in handling consumer requests), and integrity (e.g., be honest in handling transactions) (Mayer et al. 1995). Over time, the consumer trust that develops from such efforts should make it easier for these Internet businesses to elicit even more personal information from their consumers.

## Conclusion

This study builds on the existing literature by simultaneously investigating the impact of reward preferences and privacy concerns on disclosure tendency under varying levels of consumer trust. It contributes to the literature on online information privacy in several ways. First, it shows that meeting reward preferences (by providing suitable rewards) and alleviating privacy concerns (by providing suitable privacy protections) can achieve similar effects of encouraging disclosure of personal information. Second, it clarifies the role of consumer trust in this process. Consumer trust can facilitate disclosure of personal information directly or through suppressing the reward preferences and privacy concerns of consumers. In summary, besides offering some foundational elements (personal and organizational factors) that should contribute toward a theory on online information privacy, the findings of this study provide precise guidance (in the form of seven reward preferences and four privacy concerns) to Internet businesses on how they can effectively elicit personal information from their consumers.

In the future, an increasing number of Internet businesses may adopt focused marketing efforts and exploit opportunities for mass customization because this is a good survival strategy. For such efforts to be effective, these Internet businesses would need to collect plenty of personal information from consumers. Future research efforts, in the direction taken by this study, can add to our understanding about how to effectively obtain such personal information from consumers.

## References

- Bagozzi, R. P., and Yi, Y. "On the Use of Structural Equation Models in Experimental Designs," *Journal of Marketing Research* (26:3), August 1988, pp. 271-284.
- Chandon, P., Wansink, B., and Laurent, G. "A Benefit Congruency Framework of Sales Promotion Effectiveness," *Journal of Marketing* (64:4), October 2000, pp. 65-81.
- Culnan, M. J. "How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes Towards Secondary Information Use," *MIS Quarterly* (17:3), September 1993, pp. 341-361.
- Culnan, M. J., and Armstrong, P. K. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), January 1999, pp. 104-115.
- Culnan, M. J., and Bies, R. J. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2), April 2003, pp. 323-342.
- Dirks, K. T., and Ferrin, D. L. "The Role of Trust in Organizational Settings," *Organization Science* (12:4), July 2001, pp. 450-467.
- Dony, P., and Cannon, J. P. "An Examination of the Nature of Trust in Buyer-Seller Relationships," *Journal of Marketing* (61:2), April 1997, pp. 35-51.
- Hair, J. F., Anderson, R. E., Tatham, R. C., and Black, W. C. *Multivariate Data Analysis with Readings*, Prentice Hall, Englewood Cliffs, NJ, 1995.
- Hann I. H., Hui, K. L., Lee, T. S., and Png, I. P. L. "Online Information Privacy: Measuring the Cost-Benefit Tradeoff," *Proceedings of the Twenty-Third Annual International Conference on Information Systems*, L. Applegate, R. Galliers, and J. I. DeGross (eds.), Barcelona, Spain, 2002, pp. 1-10.
- Hoffman, D. L., Novak, T. P., and Peralta, M. "Building Consumer Trust Online," *Communications of the ACM* (42:4), April 1999, pp. 80-85.
- Hu, L. T., and Bentler, P. M. *Evaluating Model Fit: Structural Equation Modeling: Concepts, Issues, and Applications*, Sage Publications, Newbury Park, CA, 1995.
- Jarvenpaa, S. L., Tractinsky, N., and Vitale, M. "Consumer Trust in an Internet Store," *Information Technology and Management* (1:1), January 2000, pp. 45-71.
- Lewis, J. D., and Weigert, A. "Trust as a Social Reality," *Social Forces* (63:4), June 1985, pp. 967-985.
- Mayer, R. C., Davis, J. H., and Schoorman, F. D. "An Integrative Model of Organizational Trust," *Academy of Management Review* (20:3), July 1995, pp. 709-734.
- McKnight, D. H., Choudhury, V., and Kacmar, C. "Developing and Validating Trust Measures for E-Commerce: An Integrative Typology," *Information Systems Research* (13:3), September 2002, pp. 334-359.
- Milberg, S. J., Smith, H. J., and Burke, S. J. "Information Privacy; Corporate Management and National Regulation," *Organization Science* (11:1), January 2000, pp. 35-57.
- Nunnally, J. C. *Psychometric Theory*, McGraw Hill, New York, 1978.
- Schurr, P., and Ozanne, J. "Influences on Exchange Processes: Buyers' Preconceptions of a Seller's Trustworthiness and Bargaining Toughness," *Journal of Consumer Research* (11:4), March 1985, pp. 939-953.

- Smith, H. J. *Managing Privacy: Information Technology and Corporate America*, University of North Carolina Press, Chapel Hill, NC, 1994.
- Smith, H. J., Milberg, S. J., and Burke, S. J. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly* (20:2), June 1996, pp. 167-196.
- Stewart, K. A., and Segars, A. H. "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research* (13:1), March 2000, pp. 36-49.
- Tam, E. C., Hui, K. L., and Tan, B. C. Y. "What Do They Want? Motivating Consumers to Disclose Personal Information to Internet Businesses," *Proceedings of the Twenty-Third Annual International Conference on Information Systems*, L. Applegate, R. Galliers, and J. I. DeGross (eds.), Barcelona, Spain, 2002, pp. 11-21.
- Thibaut, J. W., and Kelly, H. H. *The Social Psychology of Groups*, John Wiley & Sons, New York, 1959.
- Tversky, A., Shmuel, S., and Slovic, P. "Contingent Weighting in Judgment and Choice," *Psychological Review* (95:3), July 1998, pp. 204-217.