



Investigating online information disclosure: Effects of information relevance, trust and risk

J. Christopher Zimmer^{a,*}, Riza Ergun Arsal^b, Mohammad Al-Marzouq^c, Varun Grover^b

^a Department of Management, 325 Reilly Hall, LeMoyne College, Syracuse, NY 13214, United States

^b Department of Management, 101 Surrin Hall, Clemson University, Clemson, SC 29634, United States

^c Department of Quantitative Methods and Information Systems, College of Business Administration, Kuwait University, Safat, Kuwait

ARTICLE INFO

Article history:

Received 24 April 2008

Received in revised form 5 March 2009

Accepted 12 December 2009

Available online 4 January 2010

Keywords:

Information disclosure

Relevance

Trust

Transaction cost economics

Theory of reasoned action

ABSTRACT

Organizations rely on customer information to design new products and offer new services. However, people should not share their personal information online. We produced and tested a model of information disclosure. While prior work focused on the effects of trust and its relationship to risk in determining intent to disclose information, we assumed that information relevance was a critical antecedent to disclosure and that both relevance and trust could alleviate perceptions of risk associated with disclosure, thereby increasing peoples' intentions to disclose information. We tested our model using 264 subjects in an experimental setting. The results showed the importance of relevance on intentions to disclose information – allowing us to draw implications for practice about voluntary information disclosure in online settings.

© 2009 Elsevier B.V. All rights reserved.

1. Introduction

Today, people demand greater product variety at lower prices, but this means that the provider needs personal information about their customers as a source of long-term competitive advantage. The online environment is particularly suitable for acquiring such information. The US FTC reported that 99% of online companies collect personal information from individuals visiting their web sites.

Ideally, collecting information and building customer profiles that provide buying patterns and behavior can create a win–win situation for both parties. However, despite the fact that more than 126 million adults in the US rely on the Web for communication, information, and shopping, they are still uncomfortable when sharing information over the Internet.

Customer information can be solicited explicitly (with surveys) or tracked implicitly (by monitoring transactions). In our study, we sought to understand customer feelings when information was explicitly solicited. We examined the question: *What are the factors that affect an individual's intent to voluntarily disclose personal information to a website?*

When engaging in e-commerce the disclosure is not voluntary. The individual *must* provide information to complete the transaction. Thus purchasing an object on line was outside the bounds of our study. Filling out an opinion survey about product preferences is, however, an example of voluntary information disclosure and it thus fell within the boundary of our study. People are aware of the inherent value of personal information and do not indiscriminately share it, though, they sometimes do. We chose to view a disclosure as a situation having a great degree of initial friction. An individual will not disclose information until the recipient (e.g., an organization) takes steps to reduce that friction. One mechanism that organizations use is trust, which often has to be extended in order to build a trusting relationship.

We took a more utilitarian view and argued that information relevance will also reduce friction allowing disclosure without having to first build trust. Individuals are suspicious when asked for irrelevant information; suspicion increases distrust by diminishing the likelihood of disclosure. Thus organizations should try to increase customer trust, they can attempt to reduce friction by requesting only relevant information.

We propose that both relevance and trust can alleviate perceptions of risk of disclosure, thus increasing intention to disclose information. We developed and tested a theoretical model using 264 subjects in an experimental setting to test our hypotheses.

* Corresponding author. Tel.: +1 315 445 4432; fax: +1 315 455 4787.

E-mail address: zimmejoc@lemoyne.edu (J.C. Zimmer).

Table 1
Disclosure and its components.

Author	Constructs
Dinev and Hart [1]	Privacy, privacy risk, Internet trust, personal Internet interest Willingness to disclose
Hui et al. [4]	Privacy, information quantity, information sensitivity
Malhotra et al. [6]	Privacy, information sensitivity, trust, risk
Metzger [11]	Information sensitivity, privacy concerns
Metzger [10]	Privacy assurances, e-tailer reputation
Metzger [9]	Website privacy protection, privacy concerns, online experience, regard for company, prior disclosure, trust for website
Pavlou [15]	Trust, risk, usefulness, ease of use
Schwaig et al. [17]	Privacy
Tang et al. [18]	Privacy, trust

2. Literature review and theory development

2.1. Theory of reasoned action

Since disclosure behavior is a voluntary, the theory of reasoned action (TRA) is an appropriate way to view it. Consistent with expectancy theory, positive or negative attitudes are formed depending on the participant's expectations of an outcome. The question then is: what are the appropriate beliefs as antecedents to these attitudes and behavior? Studies have identified numerous factors that impact intention to disclose private information to a website. As can be seen in Table 1 studies in information disclosure have focused on privacy, trust, and risk.

One way to influence disclosure is to address the consumer's privacy concerns. The US FTC has established a set of fair information practices designed to provide adequate privacy protection. Schwaig et al. surveyed the state of privacy among Fortune 500 companies [17]. While most of them had privacy policies on their homepage, very few fully protect consumer information in all aspects of the guidelines.

Another recent work in the online context is Malhotra et al.'s investigation of information privacy concerns of Internet users [6]. Their findings indicated that their concerns negatively impacted behavioral intentions to disclose information due to perceptions of trust and risk; there may, however, be other forms of belief that play a role in consumer behavior. In our study, we looked beyond privacy concerns and developed a model that examined beliefs that shaped an individuals' intent to disclose information to websites. We proposed that intent to disclose was formed by attitudes that depend on the salient beliefs of trust, risk, and information relevance. We framed these beliefs through the lens of transaction costs.

2.2. Transaction cost economics

Transaction cost theory (TCT) was used to analyze the relationship between an organization and a customer. When a person disclosed information to an organization there is a transaction cost that changed the individuals' beliefs (i.e., *transaction costs*); if organizations could implement policies that reduced these costs, they could reduce opposition to disclosure.

Transaction costs can be considered to be made of two parts: *Coordination* → the cost of exchanging information and *transaction risk* → the possibility that the other party in the transaction will not comply with its responsibilities [3]. In our study, coordination costs are minimal, since the transaction is run on the Web. We therefore focused on the risk, since a customer will not be able to make sure whether the organization will protect or release the

information. We posit that risk of information disclosure is a central belief associated with attitudes towards disclosure behavior.

Transaction risk increases with *uncertainty* due to information asymmetry among the parties. The individual disclosing information is uncertain about the seller's opportunism and the organizational security [16]. Consumers that trust the website believe that there is less uncertainty about usage of information by the organization and, in turn, this reduces transaction risk seen by the customer.

Another important factor is *asset specificity*; the transferability of the asset (information) to another transaction. If the item is highly asset specific, then it only has value in one exchange. We argue that high asset specific information could actually minimize transaction risk. In classical TCT, asset specific investments increase the risk of opportunistic behavior, increasing transaction costs. Here, we are not concerned with investments, but the signaling aspects of information during the exchange; this could lower transaction risk. By collecting information germane to the operation and content of the website (e.g. medical information at a medical website) organizations reduce the perceived risk associated with disclosure. In contrast, an organization that collects information that seems to have no relevance to the website signals higher risk to the consumer. We therefore hypothesize that the relevance of information requested from individuals mitigates the perceived disclosure risk. Fig. 1 shows our research model.

2.3. Constructs

2.3.1. Trust in a website

Trust has been rigorously investigated [2,14]. When people evince trust, they assume that the trusted party will not take advantage of them though they do not have control over the outcome. Trust can be viewed as either rational or social. The *rational view* centers on the opportunistic behavior of others. Increase in trust minimizes transaction costs because individuals must engage in less self-protection: the likelihood of opportunistic behavior is perceived to be less. The *social view* focuses on the moral duty of the individuals. They help or trust others because they perceive it to be morally appropriate. We adopted a rational view.

People today find themselves conducting transactions in uncertain e-environments. Developing and maintaining trust online is harder than in the offline, because there is little guarantee that online firms will not engage in undesirable, unethical, or opportunistic behaviors. Consequently, there is a lack of trust in technical and institutional competence or intent in protecting personal customer information [8]. An individual interacting with a website intuitively knows that it is an online expression of people in the organization and that they are responsible for any violation or breach.

McKnight and Chervany [7] developed a trust typology; they argued that disclosing personal information worried the individual because an organization tends to act in its own best interests, not necessarily delivering what was promised. This is to the opposite of *trusting belief*: implicit in them are characteristics of competence (the trustee can do what the truster needs), benevolence (the trustee cares for and will act in the truster's best interests), and integrity (the trustee will act honestly and fulfill its promises). *Trust in website* was the construct we used.

2.3.2. Risk

Risk is the product of the uncertainty of an event and the seriousness of its outcome. When the risk of a transaction increases, costs incurred in its prevention increase; consumers are also reluctant to complete online transactions due to their

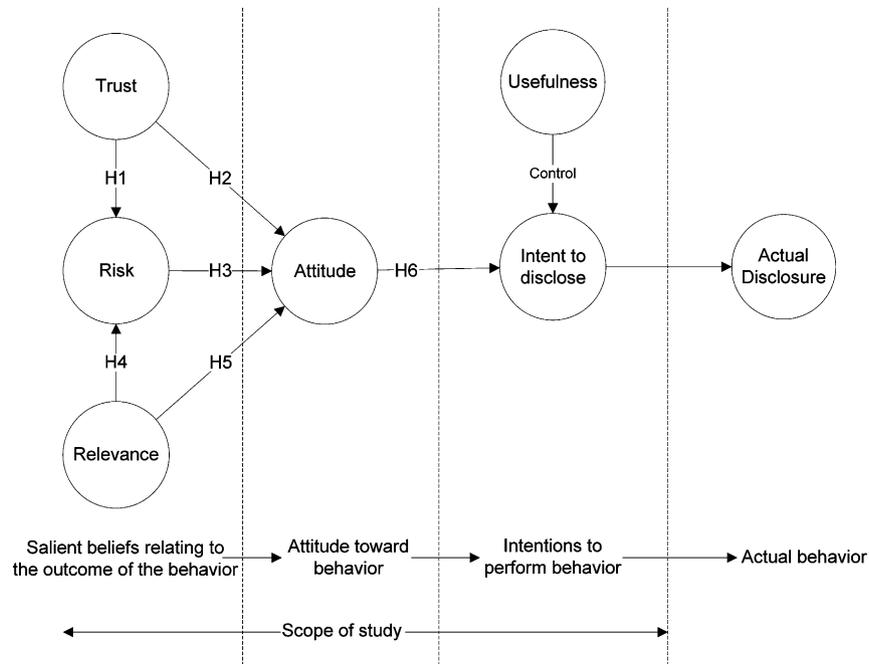


Fig. 1. Proposed research model.

Table 2
Model constructs and their definitions.

Construct	Definition
Trust in website	<i>Trusting beliefs</i> : belief that the website is benevolent, competent, or honest in handling personal information <i>Trusting intention</i> : decision to make oneself vulnerable to the website
Risk	The expectation of a high potential loss of control over the disclosed personal information to a website
Relevance	The information to be disclosed is perceived to be useful or legitimate to the function of the website
Attitude	The degree to which an individual has favorable or unfavorable evaluation or appraisal of the disclosure behavior
Intent	Individual's willingness to share her information to a website

perception of risk. We define risk beliefs (see Table 2) as the expectation of a high probability of loss of control over disclosed personal information to a website. Sharing personal information makes one vulnerable to loss of privacy, information misuse, or even identity theft, resulting in both social and financial loss.

2.3.3. Relevance

Within information science the *subjective relevance* of a document consists of topicality relevance (the way it relates to the subject of interest), cognitive relevance (how it impacts the state of knowledge), situational relevance (its pragmatic utility), and affective relevance (the emotional reaction one has to it) [19]. For our research in the context of a website requesting information from a consumer, information is relevant only if it is perceived as legitimate or useful for the function or purpose of the website (see Table 2). So, we use subjective topicality as the appropriate concept of relevance in our context.

Several authors have found that workers felt that their privacy was invaded when apparently irrelevant information was collected. The relevance of descriptive information was found to affect an individual's decision making process when presented with a choice. The information was also perceived to be more helpful based on its level of relevance.

Evidence suggests that relevance is context specific, affects perceptions of utility, and varies from one individual to another. Therefore, when a person is asked to disclose a specific piece of information to a particular website, the perception of relevance shapes beliefs regarding subsequent use (and risks) of the information after disclosure.

2.3.4. Control variable: usefulness of the website

Perceived usefulness affects individuals' intention to use IT. Our focus is not on *quid pro quo* arrangements where individuals disclose information in return for something useful but on factors that influence voluntary disclosure. We therefore controlled the direct effects of perceived website usefulness on intent to disclose. Table 2 provides a summary of the constructs used in our study and their definitions.

2.4. Hypotheses

Consumers that trust a website believe that there is more predictability regarding usage of information by the exchange party, reducing transaction risk for the consumer. We extended these concepts in a voluntary information disclosure context. We expected that trust would reduce the perceptions of risk in a voluntary context, or more formally:

H1. Trust in website will negatively influence risk perceptions of disclosing information.

Based on the transaction cost arguments, we also proposed that trust and risk will have a direct influence on attitude toward disclosure. Thus we hypothesized:

H2. Trust in website will positively influence user attitudes toward information disclosure.

H3. Risk will negatively influence user attitudes toward information disclosure.

In a disclosure situation, requested information that is perceived as non-relevant would be assumed to be used for purposes other than the stated functions of the website. This would raise transaction risk by heightening concern about negative consequences of disclosure. Consequently this would affect attitude towards disclosure negatively [10,13]. Thus we hypothesized:

H4. Relevance of information asked will negatively influence risk perceptions of disclosing information.

H5. Relevance of information asked will positively influence user attitudes toward information disclosure.

We defined intent to disclose as “an individual’s willingness to share information to a website”. Because behavioral intention is known as a reliable predictor of actual behavior, we used it as a proxy for actual disclosure behavior and further hypothesized:

H6. Attitude toward information disclosure will positively affect users’ intent to disclose information online.

3. Research method

To test our hypotheses we used a quasi-experimental methodology where participants experienced and reacted to a website. This approach allowed some control over how the participants interacted. All participants viewed the same site and first received a set of instructions for tasks designed by the research team to familiarize them with many of its features. Once the participants had completed them, participants filled out the survey.

3.1. Sample

The data for our study was gathered using an online survey administered to undergraduate students taking a management course at a large US university. Since online consumers tend to be younger and better educated than the general population, students were seen as appropriate participants and our findings had direct implications for e-business functions.

A total of 1000 students were invited to participate voluntarily in the survey. Data from 264 students were collected: a 26.4% participation rate. Respondents were assured confidentiality and screened to make sure they were familiar with computers and the Internet, and also that past experience with the target website would not compromise the results.

3.2. Measures

To measure each construct, we used previously developed and validated scales from the literature. Eleven trust items were incorporated from McKnight et al.’s paper reflecting trusting beliefs and trusting intentions. Five risk items were constructed from Jarvenpaa et al.’s [5] cross-cultural e-commerce study. Consistent with TRA, items on attitude toward disclosure and intent to disclose were reworded to be appropriate for our setting. We adapted five relevance items from Mishra et al. [12], who defined relevance as “the degree to which the product stimulus information is useful in distinguishing between objects in a choice set.” The items were reflected in questions that asked the respondents whether the information was “relevant”, “useful”, “important”, “meaningful”, or “helpful” to firms.

The initial instrument was pre-tested with eleven doctoral students and faculty. Although the respondents indicated that the instrument was generally clear, they expressed concerns about the wording of some items. We reworded them and repeated the pretest until the pretesters did not identify any further problems.

A pilot study was next conducted with 35 students. The administrators had all subjects browse the website in order to familiarize themselves with the content by having them complete specific tasks. Debriefing sessions with participants revealed a few minor issues with the instructions used to familiarize participants with the website: minor changes were made until participants indicated that they were comfortable with the content and the time required to complete the exercise and survey. The complete instrument is displayed in [Appendix A](#).

3.3. Website selection

An e-commerce website would not be suitable for our research because it has a legitimate business need for personal information from its users. We were interested in disclosure in a voluntary basis, where the protection of the individual’s information was uncertain. We also required a website that was not selling a good or service. To meet our criteria, participants were therefore shown a real *medical* website, WebMD, whose content was free of charge. It offered an online community that could be joined by individuals and in which basic information was collected (see [Appendix C](#)).

3.4. Type of information collected

WebMD has a legitimate business need: to meet it, users must disclose personal information. To test the relationship among our constructs, respondents had to state their feelings about giving the data. Because not all of the information is equally risky or sensitive, we collected data about four different types. We expected to find the same pattern of relationships regardless of information requested, but the strength of the relationships might change as a function of the sensitivity and riskiness of a particular piece of information.

We developed a list of potential parts that WebMD might legitimately request if it wanted to learn more about its users; we then grouped the list into four parts that varied in sensitivity and riskiness. The information we used in the study was e-mail address, postal address, weight, and medical history. The information varied in degree of risk without being highly risky or trivial. It could be used by WebMD to better understand its customers and improve its website; e.g., by providing articles or links on weight loss programs.

3.5. Study procedure

Before participants completed our survey, all were given a specific set of instructions, finely tuned through pre- and pilot-testing. The instructions contained a set of tasks to be completed at the WebMD site to familiarize participants with the content and have a uniform perception of trust, risk, and relevance. All participants requested information about the common cold and diabetes. These medical conditions were selected because students would be expected to know something about the common cold and could judge the information presented. Diabetes was selected because students would not be expected to be as familiar with it, but could still reasonably judge the quality of the information presented. We also directed the participants to view WebMD’s privacy policy. Accomplishing these tasks took approximately 7 min, which was deemed sufficient time to allow feelings of trust, risk, and relevance of the information to develop. After interacting with the website, the subjects were moved to an online questionnaire that was used to measure the study constructs.

4. Results

We used SEM to analyze the data. This provided us the ability to analyze the measurement model before estimating the structural

Table 3
Univariate ANOVA results.

	Risk			Relevance			Attitude		
	F	MSE	p	F	MSE	p	F	MSE	p
Item 1	103	2.05	0.0001	39	2.88	0.0001	40	2.01	0.0001
Item 2	85	1.96	0.0001	22	2.82	0.0001	42	1.92	0.0001
Item 3	98	2.21	0.0001	20	2.91	0.0001	37	2.01	0.0001
Item 4	86	1.87	0.0001	25	2.94	0.0001	43	1.90	0.0001
Item 5	68	2.24	0.0001	25	2.93	0.0001	–	–	–

model. Our unit of analysis for trust of the website, while the unit of analysis for the other constructs was the information disclosed on it. By a carefully review of the target website the research team arrived at e-mail address, postal address, weight, and medical history as items such a website could be expected to request from its users.

4.1. Manipulation checks

We expect users of the site to perceive different amounts of risk, relevance, and attitudes about disclosing each of the four different types of information.

To see if the participants perceived different amounts or risk among the information types, we conducted a MANOVA using the five risk items. Apparently, participants did perceive different levels of risk (Wilks' $\Lambda = 0.73$, $F_{(15, 2584.3)} = 21.2$, $p < 0.0001$). We then tested the relevance items in the same manner and found that participants perceived different levels of relevance among the four items (Wilks' $\Lambda = 0.87$, $F_{(15, 2584.3)} = 9.07$, $p < 0.0001$). Lastly, we tested the attitude toward disclosure and found that participants also had a mean difference in their attitude toward disclosure (Wilks' $\Lambda = 0.85$, $F_{(15, 2584.3)} = 12.7$, $p < 0.0001$). The associated univariate ANOVAs are shown in Table 3, which all had mean differences among the items for each construct.

Based on the results of the manipulation checks we were satisfied that the participants did perceive differences in the risk and relevance of the four pieces of information selected for inclusion in our study. Further we were satisfied that participants had different attitudes toward disclosing these four different pieces of information.

4.2. Validity and reliability

Before testing the hypotheses we assessed the validity and reliability of the constructs. To assess reliability we calculated the Cronbach's α for each construct and the average variance extracted (AVE). Table 4 shows the results of the reliabilities tests and the latent factor means, standard deviations, and correlations.

To assess construct validity we conducted an exploratory factor analysis with a varimax rotation of all constructs. Fourteen factors emerged corresponding to the named constructs (see Table 6 and Table 7 in Appendix B). All the items loaded onto the expected factors with only one item cross loading in excess of .40 on another factor, and only 5 items cross loaded in excess of .30. From this, we can assume that the data demonstrated good construct validity.

Despite all items loading cleanly, contrary to expectations, trust yielded a single factor instead of three. To verify that trust consists of three factors, we ran another EFA with only the trust variables included. Since we expected the three dimensions were correlated, we used an oblique rotation which allowed the factors to correlate. When analyzed alone, the three expected dimensions of trust were observed (see Table 8 in Appendix B). These results suggested that, while trust consisted of three factors, the variance between them analyzed simultaneously in the first EFA overwhelmed the within

trust variance, but that when analyzed alone, trust did factor into its three theorized factors.

4.3. Hypothesis testing

We followed a two-step approach in our analysis, where we first analyzed the measurement model then the structural model. This allowed us to test both the convergent and discriminant validity of the measurement model and the nomological validity of the structural model. We used SEM package EQS 6.1 (build 83).

4.3.1. Measurement model

To evaluate the measurement model, we created our latent factors and instead of creating causal paths, allowed all latent factors to freely covary with each other. This showed that the measurement model was valid and that the data had good convergent and discriminant validity.

We checked for multivariate normality by using a normalized kurtosis estimate, where an estimate in excess of 10 indicates nonnormality, while estimates over 20 indicates a more serious problem. The estimate for our model was 109 which clearly indicated nonnormality. We addressed this by using robust estimates which corrected for the effects of nonnormality.

In assessing the measurement model, once the effects of common method bias are removed, the Satorra–Bentler $\chi^2_{2223} = 3240$, $p < 0.0001$. The model χ^2 represents a test of the difference between an overidentified model and a just identified model. Ideally the model χ^2 would not be significant, but this test alone makes too many unrealistic assumptions about the data. A better indicator of model fit is to use the normed χ^2 (dividing the model χ^2 by its degrees of freedom). For our sample the normed χ^2 is 1.45. While no clear guidelines about a minimum acceptable value for the normed χ^2 exist, our observed value is quite low. The normed χ^2 is still susceptible to sample size effects and reliance upon it alone is not recommended in determining model fit.

To further ascertain the fit of our model, we used the comparative fit index (CFI), the Bentler–Bonnett non-normed fit index (BBNFI), and the root mean square of approximation (RMSEA). All these are robust to violations of multivariate normality and provide an accurate measure of model fit. A value of 1 for the CFI and BBNFI indicate a perfect fit, and values above 0.90 indicate an acceptable level of fit. The CFI was 0.95 and the BBNFI was 0.94 both indicating good fit. The RMSEA reflected the degree of misspecification, hence the less it is, the lower the RMSEA should be. To demonstrate good fit, the RMSEA should be less than 0.08. For our sample, the RMSEA was 0.04 demonstrating good fit. Overall the results of the measurement model showed good fit; hence it was appropriate to test the structural hypotheses.

4.3.2. The structural model

We ran another SEM model with the structural paths included. It allowed us to test the full model across the four pieces of information at the same time, despite the data being at different

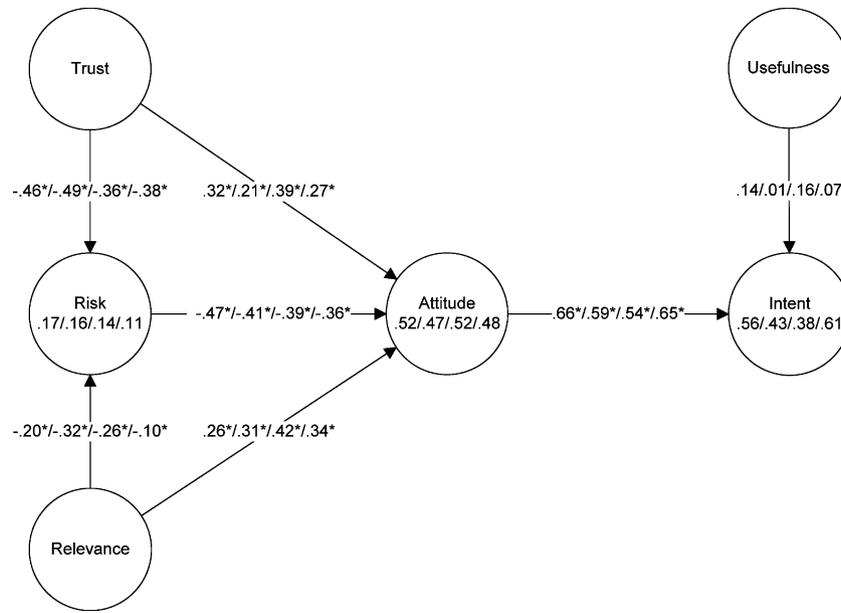


Fig. 2. Structural model results. Paths marked with * are significant ($p < 0.05$).

We then aggregated the data and retested the measurement and structural model, treating all four pieces of information as equivalent. For the measurement model, the Satorra–Bentler $\chi^2_{384} = 1680, p < 0.0001$. The normed $\chi^2 = 4.37$, which was higher than when the pieces of information were analyzed separately. The normed χ^2 was still under the upper range of a normally acceptable level. The CFI was 0.95 and the BBNFI was 0.94 both indicating good fit. Lastly the RMSEA was 0.060 demonstrating good fit. For the structural model, the Satorra–Bentler $\chi^2_{393} = 1720, p < 0.0001$. The normed $\chi^2 = 4.36$, which, like the measurement model, was higher than when the pieces of information were analyzed separately, but less than the upper range of a normally acceptable level. The CFI was 0.95 and the BBNFI was 0.94 both indicating good fit. Lastly the RMSEA was 0.060 demonstrating good fit. The structural paths for the aggregated analysis are shown in Fig. 3. All hypotheses were supported.

4.5. Limitations

One limitation relates to our sample. The literature is mixed on the suitability of using students for business research. Some argue that students fundamentally differ from the rest of the population and that generalizations beyond the student population are unwarranted. However we wished to generalize to a population using online technologies. Such consumers tend to be younger and better educated than offline consumers. However, to the extent that students do not represent typical users of WebMD or the broader population that uses websites, this sample limits generalizability of our results (Table 5).

One of the problems that researchers face is the possible existence of common method variance. It is of concern when a systematic inflation appears in the correlation of constructs matrix. To address this, we added a factor in our measurement

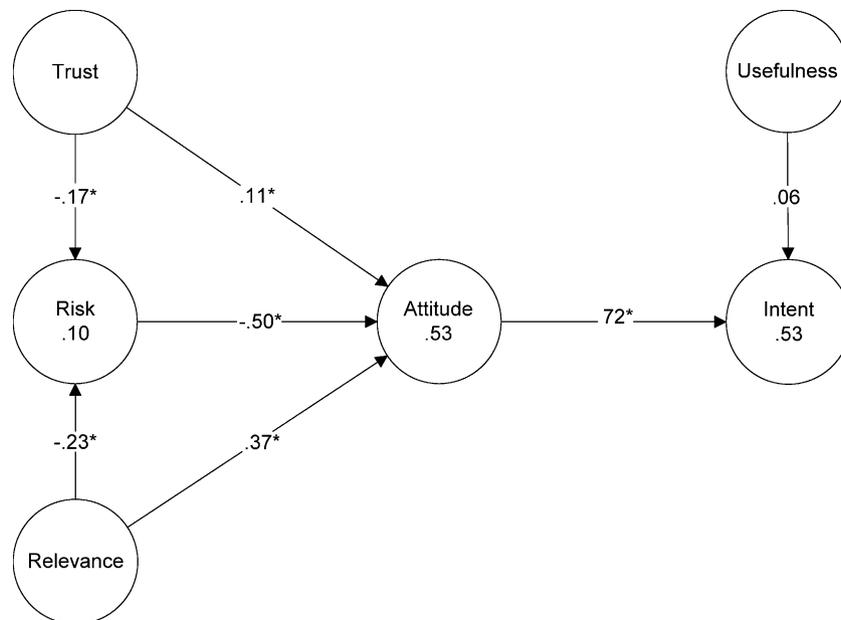


Fig. 3. Aggregated structural model results. Paths marked with * are significant ($p < 0.05$).

Table 5
Review of hypotheses.

Hypotheses	Support
H1: Trust in website will decrease risk perceptions of disclosing information.	Yes
H2: Trust in website will positively influence user attitudes toward information disclosure.	Yes
H3: Perceived risk will negatively influence user attitudes toward information disclosure.	Yes
H4: Relevance of information asked will decrease risk perceptions of disclosing information.	Yes
H5: Relevance of information asked will positively influence user attitudes toward information disclosure.	Yes
H6: Attitude toward information disclosure will positively affect users' intent to disclose information online.	Yes

and structural models that loaded on all variables, thereby addressing the possibility that a single factor could explain our findings. This did not adversely impact the results, either by causing misfit issues or significant loadings. We also used different scale anchors to address method variance. By mixing the use of Likert and semantic differential scales we used multiple methods to measure our constructs. Lastly by collecting data on four types of information, the relationships holding across all four showed that our results were robust.

Another potential limitation concerns the temporal aspects of measuring trust in website construct. We captured a static measure of trust – without formally controlling for prior familiarity with the website. The respondents generally indicated a lack of experience with Web MD and, given their age, we accepted this general assessment. However, experience with a website could have already built a trust relationship between the user and the website.

5. Discussion

The objective of our research was to understand the determinants of personal online information disclosure. Overall, our findings provided insight into the nomological network of salient beliefs that affect individuals' intent to share information with a website. The analysis of the measurement model demonstrated satisfactory validity for the instrument, while the testing of the structural model provided support to all of our hypotheses. The R^2 of 0.56 demonstrated the strength of our model.

We believe that one of our major contributions is the inclusion of information relevance. Despite the recognition of the construct in the context of information sharing, to the best of our knowledge, this is the first study in which it was tested in the nomological network of information disclosure. Our study demonstrates that information relevance directly influences the risk beliefs and the attitudes of individuals whose risk perceptions decreased and formed positive attitudes towards disclosing information when they believed that the information requested was relevant. Consistent with prior research, trust in website had a similar affect on risk and attitude.

A second contribution stems from the context of our study: prior work had investigated trust and risk in an e-commerce setting. While our context was voluntary and the removal of benefits, allowed us to observe relationships between disclosure antecedents.

5.1. Practical implications

Individuals are naturally protective of their personal information therefore the transaction risk should be minimized in order to encourage people to disclose it: organizations often incorporate trust enhancing designs disclose (displaying seals or providing links to privacy policies) to encourage it. Trust varies from person to person and with time, due to experience with promise keeping, interest congruence, etc. Asking for relevant information can help (in the short run). Our results showed that higher relevance

reduced risk perception and developed a favorable attitude toward disclosure.

6. Conclusion

Customer information is a valuable resource that can help firms achieve a competitive advantage in today's rapidly changing marketplace. Using customer information, firms strive to distinguish their products and services from the competition by better matching customer needs. Our study is a step in developing a more robust understanding of voluntary information disclosure in online settings.

Appendix A. Supplementary data

Supplementary data associated with this article can be found, in the online version, at [doi:10.1016/j.im.2009.12.003](https://doi.org/10.1016/j.im.2009.12.003).

References

- [1] T. Dinev, P. Hart, An extended privacy calculus model for e-commerce transactions, *Information Systems Research* 17 (1), 2006, pp. 61–80.
- [2] C. Flavián, M. Guinalíu, R. Gurrea, The role played by perceived usability, satisfaction and consumer trust on website loyalty, *Information & Management* 43 (1), 2006, pp. 1–14.
- [3] V. Grover, N.K. Malhotra, Transaction cost framework in operations and supply chain management research: theory and measurement, *Journal of Operations Management* 21 (4), 2003, pp. 457–473.
- [4] K.-L. Hui, H.H. Teo, S.-Y.T. Lee, The value of privacy assurance: an exploratory field experiment, *MIS Quarterly* 31 (1), 2007, pp. 19–33.
- [5] S.L. Jarvenpaa, N. Tractinsky, M. Vitale, Consumer trust in an Internet store, *Information Technology and Management* 1 (1–2), 2000, pp. 45–71.
- [6] N.K. Malhotra, S.S. Kim, J. Agarwal, Internet Users' Information Privacy Concerns (IUIPC): the construct, the scale, and a causal model, *Information Systems Research* 15 (4), 2004, pp. 336–355.
- [7] D.H. McKnight, N.L. Chervany, What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology, *International Journal of Electronic Commerce* 6 (2), 2001, p. 35.
- [8] D.H. McKnight, V. Choudhury, C. Kacmar, Developing and validating trust measures for e-commerce: an integrative typology, *Information Systems Research* 13 (3), 2002, pp. 334–359.
- [9] M.J. Metzger, Privacy, trust, and disclosure: exploring barriers to electronic commerce, *Journal of Computer-Mediated Communication* 9 (4), 2004.
- [10] M.J. Metzger, Effects of site, vendor, and consumer characteristics on web site trust and disclosure, *Communication Research* 33 (3), 2006, pp. 155–179.
- [11] M.J. Metzger, Communication privacy management in electronic commerce, *Journal of Computer-Mediated Communication* 12 (2), 2007, pp. 335–361.
- [12] S. Mishra, U.N. Umesh, D.E. Stem, Antecedents of the attraction effect: an information-processing approach, *Journal of Marketing Research* 30 (3), 1993, pp. 331–349.
- [13] N. Olivero, P. Lunt, Privacy versus willingness to disclose in e-commerce exchanges: the effect of risk awareness on the relative role of trust and control, *Journal of Economic Psychology* 25 (2), 2004, pp. 243–262.
- [14] P. Palvia, The role of trust in e-commerce relational exchange: a unified model, *Information & Management* 46 (4), 2009, pp. 213–220.
- [15] P.A. Pavlou, Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model, *International Journal of Electronic Commerce* 7 (3), 2003, pp. 101–134.
- [16] P.A. Pavlou, M. Fygenson, Understanding and predicting electronic commerce adoption: an extension of the theory of planned behavior, *MIS Quarterly* 30 (1), 2007, pp. 115–143.
- [17] K.S. Schwaig, G.C. Kane, V.C. Storey, Compliance to the fair information practices: how are the Fortune 500 handling online privacy disclosures? *Information & Management* 43 (7), 2006, pp. 805–820.
- [18] Z. Tang, Y.U. Hu, M.D. Smith, Gaining trust through online privacy protection: self-regulation, mandatory standards, or caveat emptor, *Journal of Management Information Systems* 24 (4), 2008, pp. 153–173.

- [19] X. Yunjie, Relevance judgment in epistemic and hedonic information searches, *Journal of the American Society for Information Science & Technology* 58 (2), 2007, pp. 179–189.



J. Christopher Zimmer is a Visiting Assistant Professor at Le Moyne College in Syracuse, NY. His current research interests include information sourcing, knowledge management, and individual differences in information technology (IT). He has presented his research at national and international conferences, and his work has appeared in such journals as the *Journal of Management Information Systems* and *IEEE Transactions on Engineering Management*.



Riza Ergun Arsal is a PhD candidate in the Department of Management at Clemson University. His research interests include individual adoption and use of information technologies, and behavioral issues in online settings. His work has been accepted into journals such as *IEEE Transactions on Engineering Management*, *Decision Support Systems* and the *Journal of Organizational and End User Computing*. His work has also been presented at conferences such as *Americas Conference on Information Systems (AMCIS)*.



Mohammad Al-Marzouq is an Assistant Professor in the department of Quantitative Methods and Information Systems at Kuwait University. He is a graduate of the Information Systems track of the Management PhD at Clemson University. His research focus is on privacy issues related to technology, project management, and knowledge management. Recently, his research has been targeting the Free/Libre and Open Source phenomenon.



Varun Grover is the William S. Lee (Duke Energy) Distinguished Professor of Information Systems at Clemson University. He has published extensively in the information systems field, with over 200 publications in refereed journals. Seven recent articles have ranked him among the top four researchers based on publications in the top six Information Systems journals in the past decade. Dr. Grover is Senior Editor for *MIS Quarterly*, the *Journal of the AIS* and *Database*. He is currently working in the areas of IT value, system politics and process transformation and recently released his third book (with M. Lynne Markus) on process change.