Available online at www.sciencedirect.com
SCIENCE DIRECT
Information & Management 42 (2005) 289–304
INFORMATION & MANAGEMENT
www.elsevier.com/locate/dsw

Beyond concern—a privacy-trust-behavioral intention model of electronic commerce

Chang Liu[a,*], Jack T. Marchewka[b], June Lu[c], Chun-Sheng Yu[d]

[a]Department of Operations Management & Information Systems, College of Business, Northern Illinois University, DeKalb, IL 60115 USA
[b]Department of Operations Management & Information Systems, College of Business, Northern Illinois University, DeKalb, IL 60115 USA
[c]School of Business, University of Houston, 3007 N Ben Wilson, Victoria, TX 77901 USA
[d]School of Business, University of Houston, 3007 N Ben Wilson USA, Victoria, TX 77901, USA

Accepted 3 January 2004
Available online 19 March 2004

Abstract

Despite the recent economic downturn in the Internet and telecommunication sectors, electronic commerce (EC) will continue to grow and corporate Web sites will remain an important communication channel. However, legitimate concerns regarding privacy and trust remain potential obstacles to growth and important issues to both individuals and organizations. This study proposed and tested a theoretical model that considers an individual's perceptions of privacy and how it relates to his or her behavioral intention to make an online transaction. An experiment that included over 200 subjects was conducted using two EC sites that differed only by the privacy dimensions of their notice, access, choice, and security. The results of this study suggested strong support for the model.
2003 Published by Elsevier B.V.

Keywords: Electronic commerce; Web; Privacy; Trust; Behavioral intention

1. Introduction

Over the past few years, electronic commerce (EC) has allowed organizations to enhance their economic growth, reduce barriers of market entry, improve efficiency and effectiveness, keep inventories lean, and reduce costs [29,40]. In fact, many consumers have found power in using the Internet: convenience, more choice for products and services, vast amounts of information, and time savings. They are not going to let a poor economy stop them from taking advantages of it. It is forecasted that business-to-consumer (B2C) spending will exceed US$ 95 billion in the US in 2003 and possibly US$ 250 billion by 2005. Moreover, business-to-business (B2B) online transactions now stand at more than US$ 2.6 trillion in the US, which is double the original estimate [50].

In order to achieve further growth, businesses need to understand their customers and build strong relationship with them. Today, many organizations collect customer information through registration, order, and/or survey forms, and by using ''cookies'' and tracking software to follow a customer's online activities in order to gather information about their personal interests and

* Corresponding author. Tel.: þ1-815-753-3021; fax: þ1-815-753-7460.
E-mail address: cliu@niu.edu (C. Liu).

0378-7206/$ – see front matter # 2003 Published by Elsevier B.V.
doi:10.1016/j.im.2004.01.003

preferences. This information has become extremely valuable because it allows a company to sell products and services tailored to specific customer needs. In addition, organizations can boost their revenues by selling advertising space on their Web sites because customers' personal information can be used by advertisers to better target customers [35,42].

While many customers benefit from the online information gathered about them, concerns about privacy have become an important issue and potential obstacle (e.g., [25,56,61,66]). For example, a study of Hoffman and Hoffman and Novak [30] concluded that almost 95% of the Web users they surveyed have declined to provide personal information to Web sites at one time or another. It follows that many customers may not really trust a vendor when making purchases online. Moreover, many anticipated B2B transactions and information sharing may be less effective if business partners lack trust in the Internet [52]. While opportunities to collect and use customer information to create and sustain important relationships exist, privacy concerns may limit the potential of EC transactions.

We proposed and tested a model that takes into account an individual's perception of online privacy and how it related to their level of trust in a company's electronic commerce Web site. In turn, the model suggested that trust was an important intermediary variable that influences behavioral intention for online transactions. The results of the study should be of interest to both academics and practitioners.

2. Influences of e-commerce on privacy concerns

Privacy has been defined as the right of an individual to be left alone and able to control the release of his or her personal information [64]. Concerns about privacy are not new. Businesses have collected customer information for thousands of years. However, privacy concerns often arise when new IT with enhanced capabilities for collection, storage, use, and communication of personal information come into play [10,11,13,28,44,48,59,65]. Therefore, a closer examination of the influences of EC on privacy concerns is needed to address the contemporary technological environment, as well as customer concern about the personal information collected and used by business organizations.

From a business perspective, EC applications can be classified into: business-to-consumer (B2C), intra-organizational, and business-to-business (B2B) [1]. These applications include the broad context of information exchange referred to as e-business. Privacy concerns for B2C e-commerce became an important issue because of the direct involvement of customers and the organization's potential ability to access, store, and share this personal information.

Intra-organizational applications focus on using Web technology to disseminate information internally throughout the organization. Since an intranet is an effective platform for implementing Web-based workflow and groupware, it is becoming a standard for corporate information systems [62]. Hence, greater access to data and more internal secondary data uses are needed to improve coordination within the company. However, there remains a need for managerial and technical measures to protect against loss, misuse, alteration, unauthorized access, and integrity of the data [8]. The measures may include cross-referencing data against multiple sources [53], authorization, authentication to confirm identity, non-repudiation to provide proof of origin/delivery, audit mechanisms to provide records for independent review, confidentiality to protect unauthorized disclosure, and integrity to detect unauthorized modifications [26].

EC has helped in the emergence of various virtual business relationships, including business-supplier, strategic alliance, business-client, and business-to-end-consumer [60]. Until recently, the issue of privacy was a major worry of the B2C area and privacy implications of B2B transfers had been neglected [24]. However, this is changing radically.

B2B applications now engender strong concerns about information disclosure to third parties and external secondary uses of customer personal information without the customers' consent: many state that they have a right to know what information organizations disclose to others. Moreover, many customers believe they should have the right to control their information and opt-in/opt-out to decline external secondary data use. In order to protect privacy, it is therefore necessary to address the responsibilities of both the organizations that collect personal information and the organizations that receive it secondarily [39].

Certainly organizational practice or policy will have to address these concerns in intra-organizational, B2B, and B2C contexts as new laws come into play.

In order to ease customers' concerns, organizations world-wide have begun to issue privacy policies or statements on their Web sites. These are descriptions of sites' practices for the online collection, use, and dissemination of personal information. In addition, several seal programs, such as TRUSTe^{TM}, better business bureau online seal (BBBOnLine^{TM}), and entertainment software rating board seal (ESRB^{TM}) have been developed. Privacy seals offer a readily visible and easy way to assure customers that the online business respects an individual's privacy on the Internet.

The use of privacy seals is an effort to use self-enforcement mechanisms in the exchange of accurate information and to conduct transactions. They require their licensees to abide by posted privacy policies in accordance with fair information practices and to submit to various types of compliance monitoring in order to display the specific privacy seal on their Web sites [4]. However, the question remains:

> Do privacy seals ease privacy concerns of online customers?

3. Privacy-trust-behavioral intention model

Trust becomes all the more important in a high tech environment [19]. In its absence, Web sites probably exist without loyalties. Hoffman and Novak suggest that the primary reason many people have yet to shop online or provide personal information to a vendor is due to a fundamental lack of trust with online transactions that require the customer to provide credit card and personal information.

As organizations place greater emphasis on building long-term relationships with customers, trust has assumed a central role [15,16,21,63]. A successful relationship requires businesses to describe their information collection practices and policies on its release. Customers, in turn, must be willing to provide personal information to enable businesses to advance the customer relationships through improved offerings and targeted communications [49,67].

The theory of reasoned action (TRA), [2,18,41] has been used extensively as a basis for predicting behavioral intentions and/or behaviors. The TRA contends that behavioral intentions are antecedents to specific behaviors of an individual. More specifically, an individual's attitudes and perceptions will influence that individual's actions when he or she believes that certain behavior will be linked to a specific outcome. Further, subjective norms, social pressures to perform or not perform a particular behavior influence behavioral intentions, determined by an individual's positive or negative evaluation of it. Based on the same logic, a customer's perception and attitudes regarding privacy and trust should influence his or her attitudes toward online transactions and in turn, shape his or her behavioral intentions to participate in an online business activity.

Heijden and Verhagen [27] proposed that online store image is an important predictor for the intention to purchase online. They developed reliable and valid measures which included online store usefulness, enjoyment, ease of use, store style, familiarity, and trustworthiness. Result of their study supported the assumption that trust is an antecedent of online purchase intention.

A similar conclusion can be drawn from the study conducted by Jarvenpaa et al. [33]. They suggested that consumers recognized differences in size and reputation among Internet stores, and that those differences influenced their assessments of store trustworthiness and perception of risk, as well as their willingness to patronize the store. The perception of large organizational size implies that other buyers trust the organization and conduct business successfully with it. Reputation is conceptualized as the consumer's perception of a the extent to which buyers believe a selling Internet store is honest, concerned about its customers, and can be trusted.

Although several studies addressed privacy and trust in the EC field (e.g., [7,34,43,46,51]), none have included privacy as the major antecedent of trust. In addition, little empirical research has been done to examine the relationship among the three constructs—privacy concerns, trust, and behavioral intentions. Our objective was to propose and test a theoretical model that attempted to explain how privacy influences trust and trust influences consumer behavioral intention for online transactions. This model is illustrated in Fig. 1.

Although this model is simple, it is not simplistic. The relationship is complex and required careful

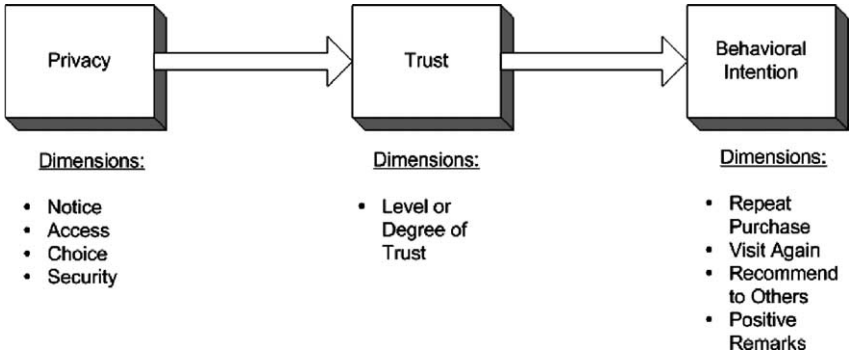

Fig. 1. Privacy-trust-behavioral intention model.

study. A model that attempted to explain everything was not feasible. Therefore, by focusing on a small component of this complex relationship, we may begin to explore and understand a complex relation- ship between consumer and firms conducting business online.

4. Research hypotheses

The US Federal Trade Commission (FTC) proposed and advocated that fair information practices included four dimensions [20]:

Notice: providing people notice that personal information is being collected prior to the collection of that information.
Access: providing people with access to the data that is collected about them.
Choice: providing people with a choice to allow an organization to use or share information collected about them.
Security: providing reasonable assurance that personal information is kept secure.

The FTC privacy dimensions provided both a practical and theoretical foundation for the privacy construct of the model. The FTC promoted adherence to these principles to insure effective privacy protection. However, a recent study conducted by Liu and Arnett suggested that only slightly more than 50% of large business Web sites provided privacy policies or appropriate links to them on their home pages. In addition, comprehensive privacy policies that addressed the four privacy dimensions were less common.

Trust has many shades of meaning [31]. It is a complex social phenomenon that reflects technological, behavioral, social, psychological and organizational aspects of interactions among various human and non-human agents. It is required when one party becomes vulnerable to the actions of another in order to perform a particular action without monitoring or controlling the other [45]. On the other hand, trust may be part of a person's personality or nature [5] that becomes forged by his or her experiences or faith in humanity [54]. Trust may also be associated with an individual's belief in an organization based upon the organization's norms, regulations, policies, and procedures [38,55,57,58]. This may be reflected in a customer's confidence in an organization offering EC transactions.

All business transactions require some element of trust, especially those conducted in the uncertain environment [37]. Customers have to trust the online business or the overwhelming social complexity will cause them to avoid purchasing [22]. In electronic commerce, trust can be viewed as a perceptual belief or level of confidence that someone respects the intentions, actions, and integrity of another party during an online transaction [32]. This perceptual belief or level of confidence represents trust as a set of specific beliefs which include integrity, benevolence, ability, and predictability of the online business [23]. Privacy protection may be an important antecedent to build trust; a customer must first believe that an online transaction will occur in a manner consistent with his or her expectations [12].

The model also suggests that the level or degree of trust an individual has will influence their behavioral

intentions. In addition to behavioral intentions of the TRA, Mehta [47] presented a model that suggested behavioral intention (such as buying interest or buying intention) was a suitable dependable variable to be used to measure the effectiveness of advertising strategy. Moreover, as Zeithaml et al. suggested, customer behavioral intention variables are the best indication of customer satisfaction and business service quality, shown by:

repeat visits to the web site;
recommendation of the web site to others;
positive remarks or comments about the web site;
repeat purchases.

Based upon the literature, the following hypotheses were used to test the proposed model:

H1.0. There is a positive relationship between privacy and the degree or level of trust an individual has when making an online transaction.

H1.1. Notification of how an organization will use personal information will have a positive relationship with respect to an individual's overall degree of trust.

H1.2. Allowing access to personal information collected about an individual will have a positive relationship with respect to an individual's overall degree of trust.

H1.3. Allowing an individual a choice to opt-in or opt-out will have a positive relationship to their overall degree of trust.

H1.4. Making reasonable attempts to keep data secure will have a positive relationship with respect to an individual's overall degree of trust.

H2.0. There is a positive relationship between the level or degree of trust an individual has with an online business and the individual's behavioral intentions.

H2.1. The degree or level of trust an individual has will be positively related to whether the individual will make an online purchase again with the online business.

H2.2. The degree or level of trust an individual has will be positively related to whether the individual will visit the online business's Web site again.

H2.3. The degree or level of trust an individual has will be positively related to whether the individual will recommend the online business's Web site to others.

H2.4. The degree or level of trust an individual has will be positively related to whether the individual make positive comments about the online business's Web site.

5. Research methodology

Our study employed a laboratory experiment. Although causality cannot be established with certainty, Emory and Cooper [17] contend that the laboratory experiment comes closer to this goal than any other research method. This allows for a higher degree of internal validity when testing the proposed model.

Research subjects included undergraduate and graduate students from a large midwestern university in the US. Over 250 subjects participated in the experiment, 212 data points were usable. Although the use of students in survey research is often criticized, they are both acceptable and appropriate when studying certain patterns of relationships [14]. Moreover, the use of students may be even more appropriate, since their demographics fit the customer profile of many online businesses.

5.1. Experimental site design and treatment group

Research subjects were randomly assigned to one of two treatment groups (High Privacy or Low Privacy) and then asked to browse the assigned Husky Virtual Bookstore (HVBS) site, view textbook requirements and descriptions, and purchase one or more books online.

Two web sites were developed for this study. One was created to include the four privacy dimensions (i.e., notice, access, choice, and security) proposed by the FTC and depicted in the proposed model. Subjects assigned to this web site were considered to be part of the High Privacy treatment group. On the other hand, the other web site did not include any of the dimensions, and subjects were considered to be in the Low Privacy treatment group.

The content of both web sites was a fictitious e-commerce bookstore that sells a variety of textbooks on-line. The first page of each storefront site included

a consent form that confirmed that the subject voluntarily agreed to participate in the study. By agreeing, the subject visited an experimental e-commerce web site and then completed a questionnaire online as part of the study. Keeping within the researchers' university guidelines on studies that involve human subjects, the subject was assured that any information gathered would remain confidential and that participation was voluntary. A button gave the subject the choice to either agree or not agree to participate. If the subject agreed and clicked the button, he or she could then continue with the study.

Next, subjects in both treatment groups were presented with an overview of three types of information that could be collected by a web site. This was to ensure that all the subjects had an understanding of how information could be collected about them, including:

Personally identifiable information: information collected through online forms, such as name, address, phone number, income, gender, age, and so forth.

Anonymous information: information that cannot be tied specifically back to a person. However, the IP address, domain names, type of browser, hardware platform, and address of the last web site visited could easily be determined by the host server.

Passive information: usually in the form of a ''cookie'' or small text file that may be sent from a server to the subject's computer. A cookie contains a unique number so that the subject's computer can be identified; however, cookies cannot search for information, transmit information to anyone else, or erase important files.

After reading this, the subject clicked a button to begin the experiment. Subjects from both the High Privacy and Low Privacy treatment groups followed the same process. This included browsing the HVBS site, viewing textbook requirements and descriptions, and purchasing one or more books with a ''false'' credit card number provided by the researchers.

The following provides a brief explanation of the High Privacy site that included the four dimensions—notice, choice, access, and security:

(1) HVBS privacy statement: provided a detailed explanation of the information that would be collected and how it would be used by the HVBS bookstore. The intent of this page was to satisfy and support the notice dimension.
(2) Main page with privacy seal: contained general information about the HVBS bookstore. This page also included a prominent privacy seal that provided a means of telling the High Privacy subject treatment group that certain standards were in place in order to increase the subjects' trust perception. In addition, a scrolling message was displayed at the bottom of the screen that assured the subject that the HVBS has taken reasonable measures to ensure data security and privacy protection.
(3) Textbook category page: contained available textbooks that included database applications, project management, operating systems, and system analysis and design. When a subject visited this page, a pop up window informed them that a electronic cookie was being down- loaded to their computer. The intent of the pop up window was to satisfy and support the notice dimension.
(4) Textbook description page: contained information specifically related to the selected book selected by the subject and included the book's description and price. After viewing this information, the subject could then add the book to their electronic shopping cart. In addition, a scrolling message at the bottom of the screen explained and enforced the perception of how security was ensured at the HVBS site. The intent was to satisfy and support the security element of the privacy principles.
(5) Shopping cart page: contained a list of books that were selected by the subject for purchase. The subject could alter the quantity or cancel the order and return to make another selection.
(6) Order registration page: collected personal information such as: name, address, telephone number, email, and so forth.
(7) Verification page: was used by the HVBS site to allow subjects to view and update their personal information. Because the site was integrated with a database management system, any changes to personal information would be immediately updated. The intention of this page was to satisfy and support the access dimension.

(8) Order processing page: supported the subject's perception that the HVBS site was secure. The subject was able to view a message that the HVBS web site uses Secure Socket Layer technology, a firewall, and stringent auditing procedures.
(9) Choice page: Before subjects left the HVBS web site, they were given the opportunity to either allow the HVBS to share the personal information they provided with external secondary sources. By allowing the subject to "opt-out," the choice dimension was supported.

5.2. Online questionnaire survey

After making an online purchase, each subject was asked to complete an online questionnaire. The data were stored in a relational database. The entire process took only about 15 min to complete. Perceptions were measured using a Likert scale ranging from 1 to 7 with "1" for strongly disagree and "7" for strongly agree. A copy of the questionnaire can be found in Appendix A.

6. Data analysis

A total of 258 subjects participated the experiment and answered the questionnaire survey. Of these, 16 were rejected because they browsed both experimental sites and answered both surveys. In order to have an equal number of the participants in both treatment groups, an additional 30 surveys were randomly selected and dropped. The final total number of subjects in this study were therefore 212, with 106 in each experimental setting group. Table 1 presents the characteristics of the student subjects.

6.1. Reliability of the measure

In order to ensure that variables in each proposed research construct (privacy, trust, and behavioral intention) were internally consistent, reliability assessment was carried out using Cronbach's a. A value within the range of 0.6–0.8 is commonly accepted as implying that variables are internally related in the manner expected [9]. Table 2 presents the research constructs, measurement, and reliability assessment. Since the internal consistency reliability coefficients for the research constructs are all above the 0.70 level, the reliability of the research constructs is supported.

Table 1
Characteristics of Respondents (N ¼ 212)

	Number	Percentage
Gender		
Male	112	52.83
Female	100	47.17
Total	212	100
Age group		
17–20	50	23.58
21-25	145	68.40
26–30	13	6.13
31–35	1	0.47
36–40	1	0.47
41–45	2	0.94
Greater than 45	0	0.00
Total	212	100
Web experience		
Never used before	4	1.89
A few times before	3	1.42
A few times/month	5	2.36
Every week	25	11.79
Almost every week	175	82.55
Total	212	100

6.2. Validity of the measure

To ensure content validity, a thorough examination was made of the relevant literature. To further reduce the possibility of non-random errors, a pretest was conducted using a group of 20 graduate information systems students to review the site design and questionnaire for validity (measuring what is intended), completeness (including all relevant variable items), and readability. Several questionnaire items were re-worded and a few Web pages were re-designed based on the pretest.

Table 2
Research constructs, measurements, and reliability assessment

Research constructs	Measure components	Cronbach's a
Privacy	Notice, access, choice, security	0.72
Trust	Level on notice_trust, access_trust, choice_trust, security_trust	0.93
Behavioral intentions	Purchase, re-visit, positive comment, recommend	0.92

Table 3
Mean values and comparing two sites with PROC TTEST

Dimension	Site with privacy dimension	Site without privacy dimension	Variable	Method	Variances	d.f.	t-Value	Pr > jtj
Notice	5.21	4.21	Notice	Pooled	Equal	210	5.69	<0.0001
Choice	5.29	3.61	Choice	Pooled	Equal	210	9.27	<0.0001
Security	5.21	3.96	Security	Pooled	Equal	210	7.09	<0.0001
Access	4.84	3.79	Access	Pooled	Equal	210	4.35	<0.0001
Trust	4.76	3.77	Trust	Pooled	Equal	210	6.20	<0.0001
Intention	5.09	4.08	Intention	Pooled	Equal	210	5.87	<0.0001

6.3. The experimental results for site differences

The experimental design consisted of two treatment groups where one site (i.e., treatment group) included the four privacy dimensions and the other did not. Table 3 summarizes the mean values from these two sites/treatment groups.

The student t-test was applied for testing the site differences of privacy, trust, and behavioral intentions. This test is especially useful for testing of differences between two groups. The null hypothesis is:

> H0: with respect to whether to incorporate privacy dimensions in site A and B, there is no difference in notice, choice, security, access, trust, and intention perceptions.

As can be seen in the lower section of Table 4, the Prob >F values are greater than 0.05, therefore we assumed that the variances were equal for the two groups. In addition, the P-values given by Prob > |t| was so small (<0.0001), that we rejected the null hypothesis and concluded that there were significant differences in customers' perceptions of notice, choice, security, access, trust, and behavioral intentions between the two sites.

In addition, a MANOVA statistical technique was applied. It measures the differences for two or more metric variables based on set of qualitative independent variables. It is useful as a multivariate procedure to access group differences across multiple metric dependent variables simultaneously. Because the data did not exhibit multivariate normal distribution, Pillai's Trace criterion technique was used. The analysis revealed a significant multivariate effect on trust toward privacy on the different web sites (Pillai's trace ¼ 0:1549, F ¼ 7:56, and P < 0:0001). In addition, the MANOVA test also revealed a significant multivariate effect on customer behavioral intention on the two different web sites (Pillai's trace ¼ 0:1970, F ¼ 8:38, and P < 0:0001).

6.4. Hypothesis testing

In testing the proposed hypotheses, mean values and a matrix of intercorrelations among the research constructs were calculated based on the 106 responses of the site with privacy dimensions. The average

Table 4
Matrix of intercorrelations among privacy and trust constructs (N ¼ 106)

Construct	Mean	S.D.	1	2	3	4	5	6
Level of trust	4.76	1.26	1.00 (0.0)					
Notice	5.21	1.32	0.64 (0.0001)	1.00 (0.0)				
Choice	5.30	1.30	0.57 (0.0001)	0.62 (0.0001)	1.00 (0.0)			
Security	5.21	1.23	0.63 (0.0001)	0.58 (0.0001)	0.62 (0.0001)	1.00 (0.0)		
Access	4.84	1.83	0.19 (0.04)	0.22 (0.02)	0.21 (0.03)	0.35 (0.0003)	1.00 (0.0)	
Overall privacy	5.14	1.06	0.64 (0.0001)	0.76 (0.0001)	0.77 (0.0001)	0.82 (0.0001)	0.67 (0.0001)	1.00 (0.0)

*Note: (1) P-values are in parenthesis. (2) The measurement scale of mean values is from 1 (completely disagree) to 7 (completely agree).

Table 5
Matrix of intercorrelations among trust and behavioral intention constructs (N ¼ 106)

Construct	Mean	S.D.	1	2	3	4	5	6
Level of trust	4.76	1.26	1.00 (0.0)					
Recommend	5.16	1.27	0.69 (0.0001)	1.00 (0.0)				
Purchase	5.10	1.54	0.62 (0.0001)	0.79 (0.0001)	1.00 (0.0)			
Visit again	5.30	1.43	0.49 (0.0001)	0.70 (0.0001)	0.75 (0.0001)	1.00 (0.0)		
Say positive	5.23	1.28	0.66 (0.001)	0.81 (0.001)	0.76 (0.001)	0.69 (0.0001)	1.00 (0.0)	
Overall intention	5.09	1.26	0.71 (0.0001)	0.91 (0.0001)	0.92 (0.0001)	0.84 (0.0001)	0.89 (0.0001)	1.00 (0.0)

Note: (1) P-values are in the parenthesis. (2) The measurement scale of mean values is from 1 (completely disagree) to 7 (completely agree).

response for the four items of trust was the measure of the overall trust value. In addition, an average for the four items of purchase, re-visit, recommend, and say positive things measured the overall customer behavioral intention. If the overall trust value was correlated positively and significantly with the four privacy dimensions, then the first set of research hypotheses could be supported. Also, if the behavioral intentions value correlated positively and significantly with the overall trust, then the second set of research hypotheses could be supported. The means, standard deviations, and matrix of intercorrelations are presented in Tables 4 and 5.

The first hypothesis (H1.1) stated that notification of how a business partner uses personal information would have a positive relationship on the degree of trust an individual will have with that business partner. The correlation coefficient was 0.64 with the P-value less than 0.0001. As the results in Table 4 suggested, a strong relationship existed.

The second hypothesis (H1.2) stated that allowing an individual to access his/her personal information would reflect a positive degree of trust. The correlation coefficient was 0.19 with the P-value less than 0.04. Therefore, there was support for this hypothesis.

Hypothesis H1.3 stated that an individual's choice to opt-out or opt-in would be positively correlated with the degree of trust that person had. The correlation coefficient was 0.57 with the P-value less than 0.0001. Consequently, strong support for this hypothesis existed.

Table 4 also provided the results for hypothesis H1.4. This suggested that reasonable attempts to keep data secure would have a positive relationship on trust. As can be seen, a correlation coefficient of 0.63 with a P-value less than 0.0001 provided support for this hypothesis.

Table 5 summarized the results of hypotheses H2.1, H2.2, H2.3, and H2.4. Hypothesis (H2.1) stated that the degree or level of trust an individual had would be positively related to whether the individual would make an online purchase again with online business. The correlation coefficient was 0.62 with the P-value less than 0.0001. As the results in Table 5 suggested, a strong relationship existed.

Hypothesis (H2.2) stated that the degree or level of trust an individual had would positively relate to whether the individual would visit the online business's Web site again. The correlation coefficient was 0.49 with the P-value less than 0.0001. Therefore, there was strong support for this hypothesis.

Hypothesis (H2.3) stated that the degree or level of trust an individual had would positively relate to whether the individual recommended the online business's Web site to others. The correlation coefficient was 0.69 with the P-value less than 0.0001. Thus, strong support for this hypothesis existed.

Table 5 also provided the results for testing hypothesis H2.4. This hypothesis suggested that the degree or level of trust an individual had would be positively related to whether the individual made positive comments about the online business's Web site. As can be seen, the correlation coefficient was 0.66 with the P-value less than 0.0001 providing strong support for this hypothesis.

These results suggest that the degree of trust is an important intermediary variable for behavioral intention. More specifically, trust is positively related to

whether an individual will purchase again, revisit a site, recommend the site to others, and make positive comments about the site.

6.5. Model testing with structural equation modeling procedures

Our model suggested that the relationships between privacy and trust and between trust and behavioral intentions are causal—perceived privacy generates positive effect on trust belief which in turn influences the behavioral intentions to continue e-commerce activities. To test this theoretical model and these causal relationships, structural equation modeling procedures were performed using AMOS 4.01.

As a first step, an exploratory factor analysis was conducted to test if the three constructs (privacy, trust, behavioral intentions) specified in the proposed model existed in the empirical data. Exploratory factor analysis using principal components extraction with varimax rotation on the items showed that all the indicators loaded onto the latent variables respectively except for one. This item was deleted from the variable list and three factors with an eigenvalue greater than one were identified, collectively explaining 67.9% of the variance.

To test the hypothesized relationships that privacy perception influenced trust, and trust, in turn, influenced consumer behavioral intention for online transactions, structural equation modeling (SEM) procedures were

Table 6
Fit indices for measurement models and standardized regression weights

Fit indices	Recommended value	Privacy model	Trust model	Intention model
w^2	N/A	19.554	17.327	7.565
P	<0.05	0.052	0.044	0.182
d.f.	N/A	11	9	5
w^2/d.f.	<3	1.778	1.925	1.513
GFI	0.90	0.951	0.950	0.972
AGFI	0.80	0.874	0.883	0.916
NFI	0.90	0.921	0.963	0.982
TLI	0.90	0.928	0.970	0.988
CFI	0.90	0.962	0.982	0.994
RMSR	0.05	0.055	0.027	0.018
Items/constructs	Privacy		Trust	Intention
Trust	0.863			
Intention			0.809	
P1	0.695			
P2	0.745			
P3	0.742			
P4	0.494			
P5	0.751			
P6	0.411			
P7	0.730			
T1			0.830	
T2			0.799	
T3			0.851	
T4			0.857	
T5			0.762	
T6			0.778	
I1				0.842
I2				0.908
I3				0.866
I4				0.748
I5				0.880

Note: minimum acceptable correlation coefficient 0.50.

adopted. This provides a means for answering two important questions with respect to support of the proposed model.

1. Does privacy perception generate a positive impact on the level of trust an individual has when making an online transaction?
2. Does the level of trust an individual has with an online business generates a positive impact on the individual's behavioral intention for online transactions?

6.5.1. Measurement model testing

To test the fit of each measurement model, a confirmatory factor analysis was first conducted using Amos 4.01. Common measures used to assess goodness of fit include w^2, degree of freedom, the w^2/d.f. ratio, goodness-of-fit (GFI), adjusted goodness-of-fit index (AGFI), normed fit index (NFI), Tucker–Lewis index (TLI, equivalent to non-normed fit Index), comparative fit index (CFI), and root mean square residual (RMSR).

According to the requirement of developing a measurement model, each latent construct must have a minimum of three indicators to be tested alone. A construct with only two indicators can only be tested together with other constructs [3]. The Privacy measurement model comprises sub-constructs of notice, choice, and security. One indicator representing access was not included, since it was excluded from the EFA test. This item was not included in any of the further SEM tests. The measures for the initial model of Privacy indicated a satisfactory fit, with a correlation of 0.45 identified between indicators P5

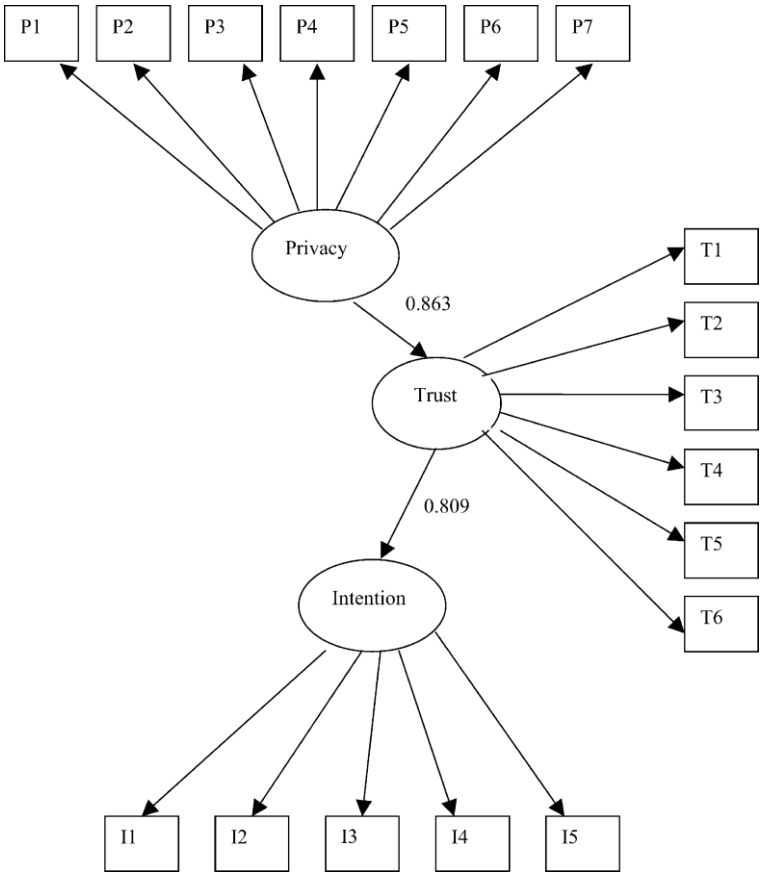

Fig. 2. The structural model for privacy, trust and behavioral intention.

(secured access) and P7 (choice to release). This may suggest some internal relationships between these two items.

All criteria indicated a good model fit for the trust measurement and behavioral intention model. Important fit indices are displayed in Table 6.

6.5.2. Path analysis

After acceptable measurement models were developed, the causal relationships among the constructs of Privacy, Trust, and Behavioral Intention were then specified and examined by performing a structural equation model test on whether the proposed conceptual framework of privacy-trust-intention provided an acceptable fit among the empirical data.

The proposed conceptual model suggested that privacy perception has a positive effect on trust which, in turn, had a positive effect on behavioral intention for online transactions. Fig. 2 shows the conceptual path model. The standardized factor loadings (correlation weights) were used to indicate the strength and direction of the relationships between the observed variables and the underlying latent variable. Compared to the minimum acceptable level of 0.50 [36], the loadings in the study showed that all observable variables but one have positive and strong relationships with the supporting latent constructs (see Table 6).

The evaluation of this conceptual path model indicated a moderate goodness of fit (w^2/degree of freedom ¼1.512, AGFI ¼ 0:797, NFI ¼ 0:873, IFI ¼ 0:953, TLI ¼ 0:942, CFI ¼ 0:952, RMSR ¼ 0:058). Although the normed fit index (NFI) value was a little lower than the commonly accepted value of above 0.90, researchers have recommended comparative fit index (CFI) as a better fit index than NFI. The CFI value for the current model was clearly above the newly revised cutoff value of 0.95. Further, the incremental indices as IFI, TLI, and CFI were believed to address the issues of parsimony and sample size known to be associated with NFI [6]. Since those indices all had values close to or above the level for superior fit (0.95), the proposed theory model was believed to have achieved a good model fit. The AGFI value appeared a bit lower but was close enough to the recommended cutoff level of 0.8. Only the RMSR value was slightly higher (>0.05). This may indicate a level of discrepancy between the sample observed and the hypothesized correlations in the theoretical model. In the theoretical model, results showed that 65% of the variance of Behavioral Intention construct was explained by the explanatory construct of trust, and 74% of the variance of trust was explained by Privacy. The empirical results concurred with the hypothetical directions. In addition, the study results indicated that privacy perception strongly influenced trust, and trust, in turn, strongly influenced behavioral intention.

7. Conclusions

Strong support exists for the theoretical model. The implications are that privacy has a strong influence on whether an individual trusts an EC business. In turn, this will influence their behavioral intentions to purchase from or visit the site again, whether they will have positive things to say about the business, and whether they would recommend this EC site to others.

Both the challenge and opportunity is to better understand individual perceptions concerning the level of trust an individual has with an electronic commerce storefront and his or her behavioral intentions. Therefore, the findings of this study should be of interest to both academics and practitioners.

However, the findings should be of interest to practitioners: having a privacy policy may lead to more repeat visits and more purchases. It would also appear that a company can increase the level of trust and a customer's behavioral intention by integrating the notice, access, choice, and security dimensions into the design of the e-commerce web site. In addition, having security controls in place and reinforcing the idea that the company is taking precautions to protect that data may be reassuring.

Although strong support for the privacy-trust-behavioral intention model exists, the authors acknowledge several limitations. First, the samples only focused on American perceptions whereas e-commerce is a global activity. Unfortunately, the experiment as a research strategy has several weaknesses and generally does not provide a high degree of external validity that would allow for drawing more general conclusions. For our study, the relatively small sample size also might influence the stability of the SEM results and thus impact the findings.

Appendix A. Online questionnaire

1. I was informed about what information the company would collect about me.
   Strongly Disagree: ° 1 ° 2 ° 3 ° 4 ° 5 ° 6 ° 7 Strongly Agree

2. The Husky Virtual Bookstore explained why they were collecting personal information.
   Strongly Disagree: ° 1 ° 2 ° 3 ° 4 ° 5 ° 6 ° 7 Strongly Agree

3. The Husky Visual Bookstore explained how they would use the information collected about me.
   Strongly Disagree: ° 1 ° 2 ° 3 ° 4 ° 5 ° 6 ° 7 Strongly Agree

4. I feel that the Husky Virtual Bookstore is making an effort to keep my personal information and credit card information out of the hands of unauthorized individuals.
   Strongly Disagree: ° 1 ° 2 ° 3 ° 4 ° 5 ° 6 ° 7 Strongly Agree

5. I feel that the Husky Virtual Bookstore will not release personal information about me without my express permission.
   Strongly Disagree: ° 1 ° 2 ° 3 ° 4 ° 5 ° 6 ° 7 Strongly Agree

6. I feel that the Husky Virtual Bookstore made a reasonable effort to ensure that the information collected about me was accurate.
   Strongly Disagree: ° 1 ° 2 ° 3 ° 4 ° 5 ° 6 ° 7 Strongly Agree

7. The Husky Virtual Bookstore gave me a clear choice before disclosing personal information about me to third parties.
   Strongly Disagree: ° 1 ° 2 ° 3 ° 4 ° 5 ° 6 ° 7 Strongly Agree

8. The Husky Virtual Bookstore has a mechanism to review and change incorrect personal information.
   Strongly Disagree: ° 1 ° 2 ° 3 ° 4 ° 5 ° 6 ° 7 Strongly Agree

9. The Husky Virtual Bookstore's policy on how it would use any personal information about me makes me feel that the company is trustworthy.
   Strongly Disagree: ° 1 ° 2 ° 3 ° 4 ° 5 ° 6 ° 7 Strongly Agree

10. The Husky Virtual Bookstore's policy with respect to how they will share my personal information with third parties makes me feel the company is trustworthy.
    Strongly Disagree: ° 1 ° 2 ° 3 ° 4 ° 5 ° 6 ° 7 Strongly Agree

11. The ability to access my personal information to ensure that it is accurate and complete makes me feel that Husky Virtual Bookstore is trustworthy.
    Strongly Disagree: ° 1 ° 2 ° 3 ° 4 ° 5 ° 6 ° 7 Strongly Agree

12. The Husky Virtual Bookstore's security policy makes me feel that the company is trustworthy.
    Strongly Disagree: ° 1 ° 2 ° 3 ° 4 ° 5 ° 6 ° 7 Strongly Agree

13. The Husky Virtual Bookstore's level of encryption and other security measures make me feel that the company is trustworthy.
    Strongly Disagree: ° 1 ° 2 ° 3 ° 4 ° 5 ° 6 ° 7 Strongly Agree

14. The Husky Virtual Bookstore's privacy policy concerning the notice of personal information collection makes me feel this company is trustworthy.
    Strongly Disagree: ° 1 ° 2 ° 3 ° 4 ° 5 ° 6 ° 7 Strongly Agree

Appendix A. (Continued)

15. After visiting the Husky Virtual Bookstore, I would be willing to provide my personal information to this site.
Strongly Disagree: ° 1 ° 2 ° 3 ° 4 ° 5 ° 6 ° 7 Strongly Agree

16. I would be willing to recommend the Husky Virtual Bookstore site to others interested in buying textbooks.
Strongly Disagree: ° 1 ° 2 ° 3 ° 4 ° 5 ° 6 ° 7 Strongly Agree

17. I would be willing to purchase from the Husky Virtual Bookstore again if I needed additional books.
Strongly Disagree: ° 1 ° 2 ° 3 ° 4 ° 5 ° 6 ° 7 Strongly Agree

18. I would be willing to visit the Husky Virtual Bookstore again.
Strongly Disagree: ° 1 ° 2 ° 3 ° 4 ° 5 ° 6 ° 7 Strongly Agree

19. I have positive things to say about the Husky Virtual Bookstore.
Strongly Disagree: ° 1 ° 2 ° 3 ° 4 ° 5 ° 6 ° 7 Strongly Agree

20. Gender: ° Male ° Female

21. To what age group do you belong?
° 17-20 ° 21-25 ° 26-30 ° 31-35 ° 36-40 ° 41-45 ° 46-50 ° over 50

22. Which statement best describe your level of experience of using World Wide Web?
° I have never used the Web before this survey
° I have used the Web a few times before this survey
° I use the Web a few times a month
° I use the Web every week
° I use the Web almost every day

References

[1] L.M. Applegate, C.W. Holsapple, R. Kalakota, F.J. Radermacher, A.B. Whinston, Electronic commerce: building blocks of new business opportunity, Journal of Organizational Computing and Electronic Commerce 6 (1), 1996, pp. 1–10.

[2] D. Albarracin, B.T. Johnson, M. Fishbein, P.A. Muellerleile, Theories of reasoned action and planned behavior as models of condom use: a meta-analysis, Psychological Bulletin 127 (1), 2001, pp. 142–161.

[3] J.L. Arbuckle, W. Wothke, AMOS 4.0 user's guide, Smallwaters, Chicago, 1999.

[4] P. Benassi, TRUSTe: an online privacy seal program, Communications of the ACM 42 (2), 1999, pp. 56–57.

[5] J. Bowlby, Attachment and Loss, Basic Books, New York, 1982.

[6] B.M. Byrne, Structural Equation Modeling with AMOS: Basic Concepts, Applications, and Programming, Lawrence Erlbaum Associates, London, UK, 2001.

[7] C. Cheung, M. Lee, Trust in Internet shopping: a proposed model and measurement instrument, in: Proceedings of the 2000 AMCIS Conference, Long Beach, CA, 2000.

[8] T. Choate, 5 Keys to customer conversion, Catalog Age, August, 2000, pp. s14–s15.

[9] G.A. Churchill Jr., A paradigm for developing better measures of marketing constructs, Journal of Marketing Research 16 (2), 1979, pp. 64–73.

[10] R.A. Clark, Information technology and dataveillance, Communications of the ACM 31 (5), 1988, pp. 498–512.

[11] M.J. Culnan, How did you get my name? An exploratory investigation of consumer attitudes toward secondary information use, MIS Quarterly 17 (3), 1993, pp. 341–363.

[12] M.J. Culnan, P.K. Armstrong, Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation, Organization Science 10 (1), 1999, pp. 104–115.

[13] G. DeSanctis, Small group research in information systems: theory and method, I. Benbasat (Ed.), From The Information Systems Research Challenge: Experimental Research Methods, Harvard Business School Research Colloquium, 1989, pp. 53–78.

[14] G.W. Dickson, A programmatic approach to information systems research: an experimentalist's view, I. Benbasat (Ed.), In the Information Systems Research Challenge: Experimental Research Methods, vol. 2, Harvard Business School Research Colloquium, 1989.

[15] P.M. Doney, J.P. Cannon, An examination of the nature of trust in buyer-seller relationships, Journal of Marketing 61 (2), 1997, pp. 31–35.

[16] F.R. Dwyer, P.H. Schurr, S. Oh, Developing buyer-seller relationships, Journal of Marketing 51 (2), 1987, pp. 11–27.
[17] C.M. Emory, D.R. Cooper, Business Research Method, fourth ed., Irwin Publisher, 1991.
[18] M. Fishbein, I. Ajzen, Belief, Attitude, Intention, and Behavior: an Introduction to Theory and Research, Addison-Wesley, Reading, MA, 1975.
[19] F. Fukuyama, Trust still counts in a virtual world, Forbes ASAP Supplement, No. 01337051, 1996, pp. 33, 69.
[20] FTC Report to Congress: Privacy online: fair information practices in the electronic marketplace, http://www.ftc.gov/os/2000/05/index.htm#22, May, 2000.
[21] E. Garbarino, M.S. Johnson, The different roles of satisfaction, trust, and commitment in customer relationships, Journal of Marketing 63 (2), 1999, pp. 70–87.
[22] D. Gefen, E-commerce: the role of familiarity and trust, Omega 28 (6), 2000, pp. 725–737.
[23] D. Gefen, E. Karahanna, D.W. Straub, Trust and TAM in online shopping: an integrated model, MIS Quarterly 27 (1), 2003, pp. 51–90.
[24] S. Goodman, Protecting privacy in a b2b world, Mortgage Banking, April, 2000, pp. 83–87.
[25] H. Green, Your right to privacy: going … going …, BusinessWeek, no. 3729, 2001, p. 48.
[26] R. Guy, Internet security: the business challenge, Telecommunications 30 (10), 1996, pp. 29–30.
[27] H.V.D. Heijden, T. Verhagen, Measuring and assessing online store image: a study of two online bookshops in the Benelux, in: Proceedings of the 35th Annual Hawali International Conference on System Sciences, Hawali, USA, 7–10 January 2002.
[28] S.C. Henderson, C.A. Snyder, Personal information privacy: implications for MIS managers, Information & Management 36 (4), 1999, pp. 213–220.
[29] R.D. Hof, S. Hamm, How e-biz rose, fell, and will rise anew, BusinessWeek, 13 May 2002, pp. 64–72.
[30] D.L. Hoffman, T. Novak, Building consumer trust online, Communications of the ACM 42 (4), 1999, pp. 80–85.
[31] D.A. Houston, Trust in the networked economy: doing business on web time, Business Horizons 44 (2), 2001, pp. 38–44.
[32] S.L. Jarvenppa, K. Knoll, D.E. Leidner, Is anybody out there? antecedents of trust in global virtual teams, Journal of Management Information Systems (JMIS) 14 (4), 1998, pp. 29–64.
[33] S.L. Jarvenpaa, N. Tractinsky, M. Vitale, Customer trust in an Internet Store, Information Technology and Management 1 (1/2), 2000, pp. 45–71.
[34] E. Kim, A Model of sustainable trust in B2C e-markets, in: Proceedings of the Seventh Americas Conference on Information Systems, Boston, MA, 2001, pp. 804–809.
[35] D. Kleinbard, Web has its eye on you, Cnnfn Financial Network, 2000, http://www.cnnfn.com/2000/03/06/technology/privacy_main.
[36] R.B. Kline, Principles and Practice of Structural Equation Modeling, The Guilford Press, New York, NY, 1998.
[37] H.G. Lee, Do electronic marketplaces lower the price of goods? Communications of the ACM 41 (1), 1998, pp. 73–80.
[38] J.D. Lewis, A. Weigert, Trust as a social reality, Social Forces 63 (4), 1985, pp. 967–985.
[39] C. Liu, K.P. Arnett, Raising a red flag on global WWW privacy policies, Journal of Computer Information Systems XXXXIII (1), 2002, pp. 117–127.
[40] G. Madden, G. Coble-Neal, Internet economic and policy: an Australian perspective, Economic Record 78 (242), 2002, pp. 343–357.
[41] T.J. Madden, P.S. Ellen, I. Ajzen, A comparison of the theory of planned behavior and the theory of reasoned action, Personality and Social Psychology Bulletin 18 (1), 1992, pp. 3–9.
[42] M. Mangalindan, Web ads on the rebound, Wall Street Journal, August 25 (2003) B1.
[43] D.M. Martin, R.M. Smith, M. Brittain, I. Fetch, H. Wu, The privacy practices of web browser extensions, Communications of the ACM 44 (2), 2001, pp. 45–50.
[44] R.O. Mason, Four ethical issues of the information age, MIS Quarterly 10 (1), 1986, pp. 4–12.
[45] R.C. Mayer, J.H. Davis, F.D. Schoorman, An integrative model of organizational trust, Academy of Management Review 20 (3), 1995, pp. 709–734.
[46] D.H. Mcknight, V. Choudhury, C. Kacmar, Trust in e-commerce vendors: a two stage model, in: Proceedings of the 21 International Conference of Information Systems, Brisbane, Australia, 2000, pp. 532–536.
[47] A. Mehta, How advertising response modeling (ARM) can increase AD effectiveness'', Journal of Advertising Research, May–June (1994) 62–74.
[48] S.J. Milberg, S.J. Burke, H.J. Smith, E.A. Kallman, Values, personal information privacy, and regulatory approaches, Communications of the ACM 38 (12), 1995, pp. 65–84.
[49] G.R. Milne, M. Boze, Trust and concern in consumers' perceptions of marketing information management practices, Journal of Interactive Marketing 13 (1), 1999, pp. 5–24.
[50] T.J. Mullaney, H. Green, M. Arndt, R.D. Hof, The E-biz surprise, BusinessWeek, May 12 (2003) 60–68.
[51] E.W.T. Nagai, F.K.T. Wat, A literature review and classification of electronic commerce research, Information & Management 39 (5), 2002, pp. 415–429.
[52] R. Preston, It's up to e-business to 'get over' privacy issue, Internetweek, 5 February (2001) 9.
[53] L. Punch, The real internet security issue, Credit Card Management 10 (9), 1997, pp. 65–67.
[54] W.H. Ricer, The nature of trust, in: J.T. Tedeschi (Ed.), Perspectives on Social Power, Aldine Publishing Company, Chicago, 1971, pp. 63–81.
[55] S. Sarker, J.S. Valacich, S. Sarker, Virtual team trust: instrument development and validation in an IS educational environment, Information Resources Management Journal 16 (2), 2003, pp. 35–55.
[56] S.D. Scalet, Checking out your shopping cart, CIO 14 (18), 2001, pp. 30–32.
[57] W.R. Scott, Organizations: Rational, Natural, and Open Systems, Prentice Hall, Englewood Cliffs, NJ, 1992.

[58] S.P. Shapiro, The social control of impersonal trust, American Journal of Sociology 93 (1987) 623–658.
[59] H.J. Smith, S.J. Milberg, S.J. Burk, Information privacy: measuring individuals' concerns about organizational practices, MIS Quarterly 20 (2), 1996, pp. 167–196.
[60] C. Speier, M. Harvey, J. Palmer, Virtual management of global marketing relationships, Journal of World Business 33 (3), 1998, pp. 263–276.
[61] M. Stepanek, Protecting e-privacy: washington must step in, BusinessWeek, July 26 (1999) EB30.
[62] E. Turban, J. Lee, D. King, H.M. Chung, Electronic Commerce: a Managerial Perspective, Prentice Hall, Upper Saddle River, NJ, 2000.
[63] J. Viega, T. Kohno, B. Potter, Trust (and mistrust) in secure applications, Communications of the ACM 44 (2), 2001, pp. 31–36.
[64] S.D. Warren, L.D. Brandeis, The right to privacy, Harvard Law Review 4 (5), 1890, pp. 193–220.
[65] J. Webster, Desktop videoconferencing: exeperiences of complete users, wary users, and non-users, MIS Quarterly 22 (3), 1998, pp. 257–286.
[66] R. Whiting, Double click gets double trouble with database plan, InformationWeek 776, 2000, pp. 24.
[67] V.A. Zeithaml, L.B. Berry, A. Parasuraman, The behavioral consequences of service quality, Journal of Marketing 60 (4), 1996, pp. 31–46.

Chang Liu, DBA, is an associate professor of management information systems at Northern Illinois University. He received his doctor of business administration from Mississippi State University in 1997. His research works published at Information & Management, International Journal of Electronic Commerce and Business Media, Journal of Global Information Management, Journal of Internet Research, Journal of Computer Information Systems, Mid-American Journal of Business, International Journal of Mobile Communications, Journal of International Technology and Information Management, and Journal Informatics Education Research.

Jack T. Marchewka is an associate professor in the Department of Operations Management and Information Systems (OMIS) at Northern Illinois University. In addition, he is also the director of the Experiential Learning Center. His current research interests include IT project management, electronic commerce, and knowledge management. His articles have appeared in Information Resources Management Journal, Information Technology and People, Journal of Global Information Management, and Journal of International Technology and Information Management.

June Lu is assistant professor teaching MBA level MIS and E-Commerce classes at University of Houston, Victoria. In addition to research on implementation of online learning systems, she conducts research on acceptance of wireless mobile technology and mobile commerce in different cultural settings. She has published in the Information & Management, Internet Research, International Journal of Mobile Communications, Journal of Computer Information Systems, Journal of Delta Pi Epsilon, and other journals. June Lu got her doctoral degree from the University of Georgia.

Chun-Sheng Yu, DBA from Mississippi State University, is assistant professor in the School of Business at the University of Houston, Victoria. His research has mainly been in cross-cultural management, quality management, and mobile commerce. Dr. Yu's articles have appeared in International Journal of Organizational Analysis, Current Topics in Management, Quality Management Journal, Journal of Internet Research, International Journal of Mobile Communications, Information & Management, and other journals.