The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0263-5577.htm

Consumer trust, perceived security and privacy policy

Three basic elements of loyalty to a web site

Carlos Flavián and Miguel Guinalíu
Faculty of Economics and Business Studies, University of Zaragoza, Zaragoza, Spain

Abstract

Purpose – The purpose of this paper is to analyze the effect of privacy and perceived security on the level of trust shown by the consumer in the internet. It also aims to reveal and test the close relationship between the trust in a web site and the degree of loyalty to it.

Design/methodology/approach – First, there is an explanation of the main attributes of the concepts examined, with special attention being paid to the multi-dimensional nature of the variables and the relationships between them. This is followed by an examination of the validation processes of the measuring instruments.

Findings – Specifically, the study reveals that an individual's loyalty to a web site is closely linked to the levels of trust. Thus, the development of trust not only affects the intention to buy, as shown by previous researchers, but it also directly affects the effective purchasing behavior, in terms of preference, cost and frequency of visits, and therefore, the level of profitability provided by each consumer. In addition, the analyses show that trust in the internet is particularly influenced by the security perceived by consumers regarding the handling of their private data.

Practical implications – The results of this study provide several managerial implications for companies in this sector. Suggestions are offered for national and international organizations involved in regulating these markets.

Originality/value – The results of this research remedy, to a certain extent, the scarcity of empirical studies that have designed and validated measuring scales for the concepts of privacy, security, trust and loyalty to the internet, as well as testing the relationships between them.

Keywords Internet, Trust, Data security, Privacy, Customer loyalty

Paper type Research paper

1. Introduction

The increasing use that organizations are making of new technologies, aimed at obtaining and processing data regarding consumer characteristics and behavior, has meant that consumers are very concerned about the use, treatment and potential transfer of their private data, as well as security in information systems (Harris Interactive, 2002; European Commission, 2004; Kelly and Erickson, 2004). Furthermore, the constant references in the media that call into question the supposed security of the internet (e.g. the spreading of viruses or hacker attacks) only serve to aggravate the already low confidence that consumers have with regard to online purchasing (Consumers Union, 2002; Emarketer, 2004). For example, over 40 percent of consumers feel that their privacy is jeopardized, with over 45 percent

The authors are grateful for the financial support of the Ministry of Education and Science and the Aragón Government (S-46; PM-034).

Industrial Management & Data Systems
Vol. 106 No. 5, 2006
pp. 601-620

0263-5577
DOI 10.1108/02635570610666403

believing that the laws currently governing the internet do not go far enough. This concern regarding the possible lack of privacy in online transactions is becoming a major obstacle to the spread of e-commerce (Lardner, 1999), due basically to the loss of control perceived by the user over the use of personal information supplied to the seller (Hoffman *et al.*, 1998).

The problems of privacy, security, and their effect on trust and loyalty on the internet have been analyzed in various research studies (Kruck *et al.*, 2002; Gavish and Gerdes, 1998). This work analyzes the influence exercised by consumer-perceived privacy and security on the trust shown to a web site, as well as the role of these variables in loyalty. First, there is an explanation of the main attributes of the concepts examined, with special attention being paid to the multi-dimensional nature of the variables and their relationships. This is followed by an examination of the validation processes of the measuring instrument (the measurement scales are shown in the Appendix, Table AI). The proposed hypotheses are tested. The work concludes with a discussion of the main managerial implications, as well as the future research lines.

2. Analysis of the concept of trust

2.1 Trust in marketing

The importance of trust in marketing is constantly growing (Sahay, 2003). Indeed, trust is considered to be, along with commitment, communication and satisfaction, one of the basic pillars supporting the relationship marketing theory. Trust may be defined as:

> . . . one party's belief that its needs will be fulfilled in the future by actions undertaken by the other party (1).

Thus, trust is a set of beliefs held by a consumer as to certain characteristics of the supplier, as well as the possible behavior of the supplier in the future (Ganesan, 1994; Coulter and Coulter, 2002). In line with this reasoning, the literature has identified various dimensions in trust. Of these dimensions, perceived honesty and benevolence have most often been associated with consumer trust. Honesty (or credibility) indicates the certainty the consumer has in the business' sincerity and the fact that it keeps its promises (Gundlach and Murphy, 1993). Benevolence is related to the consumer's belief that the company is interested in his welfare, that it does not intend to show opportunist behavior (Larzelere and Huston, 1980), and that it is motivated by the quest for joint benefit (Doney and Cannon, 1997).

2.2 Consumer trust in a web site

The constant development of relationships over the internet is significantly affecting most commercial sectors (Gunasekaran and Love, 1999; van der Smagt, 2000; Wu and Chang, 2005; So *et al.*, 2005). However, this influence has not been translated into high sales figures via the internet since there is a lack of trust that means that consumers are reluctant to adopt e-commerce (Gefen, 2000; Jarvenpaa *et al.*, 2000; So and Sculli, 2002; Hedelin and Allwood, 2002). This distrust is a consequence of the particular features of the internet when set against transactions conducted via traditional channels (Yousafzai *et al.*, 2003). Thus, when a consumer conducts a transaction with an online store that is characterized to be operating in an uncertain environment (Fung and Lee, 1999) such as the internet, the consumer is less likely to trust that everything about his transaction is assured and normal as compared to his transactions with an offline store.

In this respect, it is clear that with online transactions the consumer has no physical interaction with the seller, and therefore, is unable to evaluate effectively the products on offer or check the identity of the seller. Furthermore, payment is usually made by credit card prior to the delivery of the goods or services, making it possible for the consumer's financial data to be used fraudulently. It is also possible that the product received is not the one that was ordered. To this it must be added the difficulty in making complaints to companies that have no physical presence or whose head office is in another country, and the fact that some consumers are barely internet-savvy so that they cannot distinguish between the alternatives. In addition we have to note the increasing problem with spam, the continuous periodic reports on hacker attacks and viruses; and the existence of a legal framework that is incomplete, heterogeneous and ineffective. In short, it would be fair to say that the risks the internet consumer appears to have to face are extremely high (Koufaris and Hampton-Sousa, 2002). Indeed, internet purchases are perceived as being riskier operations (Taylor Nelson Sofres Interactive, 2002), and the development of trust via the internet is more difficult than in the traditional channels (Bitting and Ghorbani, 2004).

In addition, the particular characteristics of online purchasing mean that the study of trust needs to include aspects beyond those traditionally considered in marketing literature. In this respect, we should point out that while a good many researchers limit the number of dimensions making up trust to perceived honesty and benevolence, some authors have considered that it also depends on other factors, such as perceived competence (Sirdeshmukh *et al.*, 2002). This dimension refers to the skill and ability perceived in the other party. Thus, it is a set of abilities and characteristics that enable a person or organization to exert influence in a specific activity (Mayer *et al.*, 1995), and therefore, meet its commitments (Sako and Helper, 1997). Perceived competence is particularly important in particular contexts, such as the internet (Suh and Han, 2003; Roy *et al.*, 2001). The reason for this is that the internet businessman needs to prove beyond doubt that as well as being honest and acting in good faith, he has the technical, financial and human resources needed for completing the transaction successfully, such as meeting the delivery date, or making sure that any banking details stored are kept confidential. In other words, it is not only a question of making promises and having good intentions, but also ensuring that these promises and intentions really materialize. For this reason, as this work analyzes the role of trust in the internet purchasing behavior, trust is considered to be made up of three basic dimensions: the web site's perceived honesty, benevolence and competence.

3. The influence of privacy and perceived security on internet consumers' trust and loyalty

This work proposes a model that relates trust, privacy and security with the loyalty shown to a web site. With this in mind, we also shall review the concepts of privacy and security, which are two of the aspects most often related to trust in online relationships. We shall then analyze the close link between them and the influence they have on web site users' trust and loyalty.

3.1 Privacy

The concept of privacy is in itself not new and it has generally been defined as an individual's ability to control the terms by which his personal information is acquired

and used (Westin, 1967; Galanxhi-Janaqi and Fui-Hoon Nah, 2004). Where the internet is concerned, privacy affects aspects such as the obtaining, distribution or the non-authorized use of personal information (Wang *et al.*, 1998). New technologies' growing capacity for information processing, plus its complexity, have made privacy an increasingly important issue (Kelly and Erickson, 2004, 2005). Consequently, consumer distrust is increasing regarding how their personal data is being gathered and processed. The quantitative importance of this issue is shown by Udo (2001), who points out that the protection of privacy is the greatest concern of internet purchasers.

3.2 Security

As well as problems with the lack of privacy, the lack of security as perceived by online consumers is another of the main obstacles to the development of e-commerce (Furnell and Karweni, 1999; Chou *et al.*, 1999; Dong-Her *et al.*, 2004). The reason for this is the possibility that financial data might be intercepted and put to fraudulent use (Jones *et al.*, 2000). Kolsaker and Payne (2002) maintain that security reflects perceptions regarding the reliability of the payment methods used and the mechanisms of data transmission and storage. Perceived security may be defined as the subjective probability with which consumers believe that their personal information (private and monetary) will not be viewed, stored, and manipulated during transit and storage by inappropriate parties in a manner consistent with their confident expectations. Thus, what we are talking about here are the technical aspects that ensure the integrity, confidentiality, authentication and non-recognition of transactions. The integrity of an information system refers to the impossibility of the transmitted or stored data being modified by third parties without permission. Confidentiality involves the data being seen by authorized individuals. Authentication allows a certain operation to be carried out only after identification, or if there are guarantees of the identity of the party one is dealing with (e.g. a web site). Finally, non-repudiation refers to procedures that prevent an individual or organization from denying that they had carried out a certain operation (e.g. a purchasing order).

3.3 The relationship between perceived privacy and security on a web site

The analysis conducted above shows that although the privacy and security variables in internet relationships are related, they have particular characteristics that enable us to establish a clear distinction between them. Specifically, privacy is linked to a set of legal requirements and good practices with regard to the handling of personal data, such as the need to inform the consumer at the time of accepting the contract what data are going to be collected and how they will be used. Security refers to the technical guarantees that ensure that the legal requirements and good practices with regard to privacy will be effectively met. For example, the company may promise that the data will not be given to third parties without the consumer's consent. Yet hackers might get hold of the data and hand them over to malefactors. This invasion of privacy can only be prevented by the use of suitable security measures. The close relationship between the concepts of privacy and security may be seen in three clearly distinct areas. First, it should be emphasized that there is a close relationship between the two concepts in the mind of consumers. Indeed, at times consumers do not make a clear distinction as to where one concept ends and the other begins, and they may well confuse them. Usually, this distinction is not particularly relevant for consumers, since

all they want is that their privacy be respected, either through the law, good practices, secure systems or a combination of the three. Second, it is worth pointing out that companies tend to handle both concepts jointly. In fact, the idea is widely spread in the business world that protection of privacy is an element that depends not only on the following of a series of behavior guidelines or the law; it also depends on the reliability of information systems (Lyman, 2003). Third, we see that public bodies view both concepts as running side by side. Thus, legislative measures include, along with those of a procedural nature regarding the collection, use and transfer of private data, others of a purely technical nature (e.g. Directive 2002/58/EC of the European Parliament and of the Council, of 12th June 2002 (European Commission, 2002), concerning the processing of personal data and the protection of privacy in the electronic communications sector).

Thus, it seems fair to say that in view of the particularities of the privacy and security variables, the two need to be handled as distinct concepts. However, as we have seen, not only the consumer, but also the company and the legislator perceive that the two concepts have a close relationship. This suggests the need for the two variables to be dimensions of a single construct. This construct, called perceived security in the handling of private data (SHPD), shows the consumer's perception of practices regarding personal data protection carried out by the web site, and the security of the information system in which these practices are to be found.

4. Working hypotheses

Several authors have analyzed the precursory factor of online trust. For example, Lee and Turban (2001) suggest that merchant integrity is a major positive determinant of consumer trust in internet shopping, and that its effect is moderated by the individual consumer's trust propensity. In view of the possible connection between trust and the perceived private data handling security construct, a direct relationship might be established between the two concepts. In fact, recent studies suggest a possible link between the low level of trust in relationships established over the internet and the high level of concern regarding consumers' privacy and security. For example, a recent study conducted in the European Union (European Commission, 2004) showed that only 23 percent of European online purchasers fully trusted the internet as a purchasing channel. The figures are particularly alarming for countries such as Spain and Portugal, with only 9 and 13 percent, respectively, showing a complete degree of trust. The subjects clearly showed that security when paying was the aspect that most concerned them, with levels reaching 48 percent. Similar figures are to be found in the USA, with a study by Harris Interactive (2002) showing that the three main sources of distrust are:

(1) that companies might transfer personal data to others without express consent;

(2) transactions might not be secure; and

(3) hackers might steal personal information.

Without a doubt, this connection between the concepts of trust and perceived security in personal data handling is plausible and worthy of examination in greater detail. Thus, we propose that perceived privacy and perceived security are antecedents of trust developed due to the nature of the internet. With the aim of testing whether this connection is widespread, the following hypothesis is proposed:

H1. The greater consumers' perception of security with regard to the handling of their personal data, the greater their trust in a web site.

In this work, loyalty is defined as preference for a particular web site. This preference causes the web site to be the one that is visited most and is chosen for the purchase of a certain product category. These three elements – preference, visiting frequency and amount spent – were measured for three items. Certain authors (Goldman, 1978) have shown that consumers are more loyal to establishments that give them most reason to trust them. This loyalty is explained by a strategy of risk reduction by the consumer, whereby it is preferable to stay loyal to an establishment that has shown its trustworthiness in the past, rather than risk looking for alternatives (Assael, 1992). This reasoning can be extended to online commercial relationships, where it has been noticed that lack of trust is one of the main obstacles to the spread of e-commerce. In this respect, it is worth noting that certain merely descriptive studies show that 49 percent of consumers are reluctant to make their purchases over the internet due to the high degree of mistrust they feel (Truste, 2003). These results suggest that loyalty to a web site depends to a great extent on the consumer's trust shown towards it (Lee *et al.*, 2000; Quelch and Klein, 1996), since there tend to be greater levels of risk associated with this type of distance dealing (Donthu and Garcia, 1999). Chircu *et al.* (2000) show that trust and expertise become more important in determining the adoption intention as transaction complexity increases. Consumer trust is as important to online commerce as the widely accepted TAM use-antecedents, perceived usefulness and perceived ease of use. According to Gefen *et al.* (2003), these variable sets explain a considerable proportion of variance in intended behavior. It is, therefore, reasonable to suggest that greater levels of trust will lead to improved consumer loyalty to a web site.

H2. The greater the consumer's trust in a web site, the greater the loyalty towards it.

The number of consumers who make purchases via the internet is currently very low. For example, in the European Union, only 16 percent of internet users admit to having made some purchase online (European Commission, 2004). Among reasons given by consumers to explain their low expenditure rates on the internet, the most frequent are insecurity and lack of protection for their privacy. In this respect, according to Taylor Nelson Sofres Interactive (2002) there are two major reasons why consumers do not purchase online:

(1) unwillingness to give out data regarding their credit cards; and

(2) the idea that it is safer to buy in physical stores than online.

Similarly, CIB (2003) says that spam is the second largest barrier to internet purchasing after shipping costs. Consequently, it seems reasonable to suggest that the security the consumer perceives in the handling of his personal data by the web site will have a direct influence on his loyalty.

H3. Increased consumers' perception of security with regard to the handling of their personal data will result in an increase in the loyalty shown to the web site.

5. Validation of the measuring scales

Data were collected through a web survey using Spanish-speaking subjects. This group of internet users is relevant due to the fact that Spanish is the fourth language on the internet after English, Chinese and Japanese (see www.internetworldstats.com). In order to obtain the responses several banners and posts were included on heavy traffic online media web sites, e-mail distribution lists and well-known electronic forums. The selection of the media to promote the research was founded on:

- the level of awareness among the Spanish-speaking community;
- traffic level; and
- availability.

To value the level of awareness and traffic, we collected the opinion of four experts on e-marketing (two well-recognized practitioners and two academics specializing in new technologies and electronic commerce) and the rankings offered by the specialized firm Nielsen//NetRatings and Google. The experts compounded the promotional medium set according to the three criteria above, the mentioned rankings and their experience in the field. One of the most important Spanish online newspapers was selected. Moreover, we posted in several Usenet groups and electronic forums, all of them well-known, visited frequently by the Spanish-speaking community and related to different topics, such as purchasing, leisure, social networks or professional activities. Banners were published for one month. Posts were realized twice in a month. Potential interviewees were linked to a specific web site where they could obtain all the information about the research project. Questionnaires were to be returned by e-mail, fax or mail. Likewise a raffle was held among participants who returned the questionnaire correctly.

We followed the recommendations of Roberts *et al.* (2003) – to allow subjects to choose the web site to analyze – due to the fact that the objective of this work was to understand online consumer behavior regardless of what type of product or service was being distributed. However, it was required that the subject had made acquisitions through the web site selected several times per month during the previous year. The results obtained were satisfactory, with approximately 400 responses, which, once sifted because of the existence of repetitions, atypical cases or empty responses, were reduced to 354. In qualitative terms, the representativity of the sample was high, due firstly to the great variety of product categories analyzed (financial services, auctions, books, music, travel, hardware and software, news, clothes, food) and second, to the fact that the average profile of the subjects coincided with the results of other research studies (Forrester Research, 2001). The subjects were mostly male (67.2 percent), aged between 25 and 34 (53.1 percent), with a high level of education (81.2 percent had pursued tertiary studies), over 5 years' experience in the use of computers (87.5 percent), somewhat less in the use of the internet (44.5 percent), and a high frequency of access to the web (83 percent logged on several times a day). These data are similar to the sociodemographical characteristics of the Spanish internet user (AECE, 2005; AIMC, 2005).

We used the statistical analysis packages SPSS v. 13 and EQS v. 6.1. Cronbach α data were satisfactory (honesty = 0.916; benevolence = 0.893; competence = 0.852; privacy = 0.926; security = 0.953; loyalty = 0.767). The descriptive data of the items are shown in Table I.

5.1 Confirmatory factor analysis

As we can observe in Table I, normality of the data is not guaranteed. As a consequence we opted to use the method of robust maximum likelihood, since it affords more security in samples, which do not unmistakably pass multivariate normality tests. We carried out a confirmatory model development strategy (31), following the criteria set by Jöreskog and Sörbom (1993) and Lozano (2002):

- the weak convergence criterion (Steenkamp and Van Trijp, 1991) means eliminating indicators that do not show significant factor regression coefficients (t student >2.58; $p = 0.01$);
- the strong convergence criterion (Steenkamp and Van Trijp, 1991) involves eliminating non-substantial indicators, that is to say, those whose standardized coefficients are lower than 0.5 (Hildebrant, 1987);
- Jöreskog and Sörbom (1993) also suggest eliminating the indicators that contribute least to the explanation of the model, taking as a cut-off point $R^2 < 0.3$ (Flavián and Lozano, 2003); and
- eliminate items with a lower R^2 value, when the model fit is not acceptable (Lozano, 2002).

The results were satisfactory. However, as an extra measure, we calculated the values of the average variance extracted or AVE (Jöreskog, 1971), and the composite reliability or CR (Fornell and Larcker, 1981). The results were satisfactory, being above the recommended minimum of 0.5 and 0.7 (AVE-CR): honesty (0.56-0.87), goodwill (0.48-0.85), competence (0.50-0.80), privacy (0.53-0.89), security (0.58-0.92), loyalty (0.51-0.76).

Finally, in order to confirm the existence of multi-dimensionality in the trust and perceived security in the handling of personal data variables, a rival models strategy was developed (Hair *et al.*, 1998; Anderson and Gerbing, 1988). For this, we compared a second-order model in which various dimensions measured the multi-dimensional construct under consideration, with a first-order model in which all the items weighed on a single factor (Steenkamp and Van Trijp, 1991). The results showed that the second-order model was a much better fit than the first-order model (see Table II, models 1TRUST and 2TRUST, and 1SHPD and 2SHPD). These results led us to conclude that both variables showed a marked multi-dimensional nature.

5.2 Validity analyses

5.2.1 Content validity. In the case of trust we considered the works of Kumar *et al.* (1995), Siguaw *et al.* (1998), Doney and Cannon (1997) and Roy *et al.* (2001); for privacy, Janda *et al.* (2002), O'Cass and Fenech (2003) and Cheung and Lee (2001); for security,

Table I. Univariate statistics

Variable	PRIV	SEC	HON	BEN	COM	LOY
Mean	5.6798	5.4098	5.6469	5.4483	5.8084	5.4680
Skewness (G1)	−1.3155	−0.8371	−0.9469	−0.7928	−1.3845	−1.0420
Kurtosis (G2)	2.2153	0.2246	1.3757	1.0300	3.5303	0.5890
Standard dev	1.1631	1.2580	1.0532	1.0252	0.9390	1.4132

and O'Cass and Fenech (2003); and for loyalty, Rowley and Dawes (2000), Nilsson and Olsen (1995), Yoon and Kim (2000) and Flavián *et al.* (2001). However, it was necessary to adapt these scales. The draft scales were presented to a focus group made up of various independent experts in such fields as marketing, the internet and new technology law. Moreover, a quantitative pre-test of an exploratory nature was given to a sample of 30 consumers.

5.2.2 Convergent validity. Convergent validity was tested by checking the confirmatory model to see that the loads of the various indicators were statistically significant (level of 0.01) and higher than 0.5 points (Sanzo *et al.*, 2003). In addition, in the case of the multi-dimensional variables, we checked that the correlations between the various dimensions proposed were significant (level of 0.01) and high (Table II).

5.2.3 Discriminatory validity. First, the correlation between the variables in the confirmatory model was tested to ensure that they were not much higher than 0.8 points (Bagozzi, 1994). Second, we checked that the value 1 did not appear in the interval of trust of the correlations between the different variables. Finally, the correlation between each pair of variables was set at 1 and a χ^2 differences test was carried out (Bagozzi and Yi, 1988). The results showed an acceptable level of discrimination (Table III).

6. Testing of hypotheses

In the testing of the structural model, each of the dimensions corresponding to trust and perceived SHPD was replaced by its arithmetical mean (method of parceling). This is a common practice among researchers (Roberts *et al.*, 2003), which can only be done provided the correct fit of a second-order factorial model has been checked.

With regard to the results of the structural model, we saw that the direct effect of perceived security in private data handling (the SHPD variable in Figure 1) on consumer trust was significant (level of 0.01) and positive, and so hypothesis *H1* was accepted. Moreover, the R^2 for trust was particularly high. Second, we observed that trust had a clear positive effect on loyalty to a web site, and so hypothesis *H2* was accepted. However, hypothesis *H3* had to be rejected because although the estimated parameter had the expected sign, it was not statistically significant (level of 0.01). This result showed us the mediating role played by trust in the relationship between perceived security in private data handling and loyalty to a web site. Finally, mention should be made of the notable fit obtained in the structural model (Table IV).

7. Conclusions, managerial implications and future research lines

In previous literature, several authors have distinguished the important role of consumer trust for the success of electronic commerce (Fung and Lee, 1999; Chircu *et al.*, 2000). Thus, Chircu *et al.* (2000) investigate how the degree of online consumer trust in an electronic commerce intermediary and the level of expertise that the consumer needs in order to be able to use the intermediary affect the intention to adopt the electronic commerce intermediary. In addition, Lee and Turban (2001) describe a theoretical model to study the four main influences on consumer trust in internet shopping: trustworthiness of the internet merchant, trustworthiness of the internet as a shopping medium, infrastructural (contextual) factors (e.g. security, third-party certification), and other factors (e.g. company size, demographic variables). However, considering the significant importance of this topic, more empirical research is needed in this area.

Table II.
Confirmatory factor analyses

Indicator	Recommended value	1TRUST value	2TRUST value	10SHPD value	20SHPD value
Absolute fit					
χ^2	$p > 0.05$	943.843, 91 gl $p < 0.001$	434.566, 88 gl $p < 0.001$	1,338.057, 90 gl $p < 0.001$	885.340, 89 gl $p < 0.001$
Satorra-Bentler χ^2	$p > 0.05$	575.6065; $p = 0.0000$	285.8330; $p = 0.0000$	691.8934; $p = 0.0000$	473.4507; $p = 0.0000$
RMSEA	RMSEA < 0.8	0.163	0.106	0.198	0.159
GFI	Close to 1	0.676	0.855	0.587	0.699
Incremental fit					
NFI	NFI > 0.9	0.761	0.890	0.760	0.841
NNFI	NNFI > 0.9	0.744	0.892	0.733	0.828
AGFI	Close to 1	0.572	0.803	0.449	0.594
CFI	Close to 1	0.778	0.910	0.771	0.854
RCFI	Close to 1	0.715	0.884	0.773	0.847
IFI	Close to 1	0.779	0.910	0.772	0.855
Parsimony fit					
Normed χ^2	(1; 5)	10.371	4.938	14.867	9.948
PNFI	Maximum	0.659	0.746	0.651	0.713

	Correlations	Confidence interval	χ^2 differences
HON-BEN	0.77*	(0.71; 0.83)	239.797 (gl = 1; $p < 0.01$)
HON-COM	0.68*	(0.58; 0.77)	160.674 (gl = 1; $p < 0.01$)
HON-PRIV	0.61*	(0.50; 0.61)	135.872 (gl = 1; $p < 0.01$)
HON-SEC	0.51*	(0.42; 0.61)	93.549 (gl = 1; $p < 0.01$)
HON-LOY	0.39*	(0.26; 0.52)	42.569 (gl = 1; $p < 0.01$)
BEN-COM	0.82*	(0.76; 0.88)	256.537 (gl = 1; $p < 0.01$)
BEN-PRIV	0.65*	(0.56; 0.75)	157.163 (gl = 1; $p < 0.01$)
BEN-SEC	0.57*	(0.48; 0.66)	114.1 (gl = 1; $p < 0.01$)
BEN-LOY	0.39*	(0.26; 0.52)	41.983 (gl = 1; $p < 0.01$)
COM-PRIV	0.62*	(0.50; 0.73)	130.373 (gl = 1; $p < 0.01$)
COM-SEC	0.55*	(0.45; 0.65)	100.688 (gl = 1; $p < 0.01$)
COM-LOY	0.36*	(0.24; 0.49)	35.417 (gl = 1; $p < 0.01$)
PRIV-SEC	0.81*	(0.76; 0.86)	303.681 (gl = 1; $p < 0.01$)
PRIV-LOY	0.38*	(0.25; 0.51)	41.31 (gl = 1; $p < 0.01$)
SEC-LOY	0.34*	(0.23; 0.46)	34.182 (gl = 1; $p < 0.01$)

Note: *Coefficients significant to a level of 0.01

Table III.
Convergent and discriminatory validity

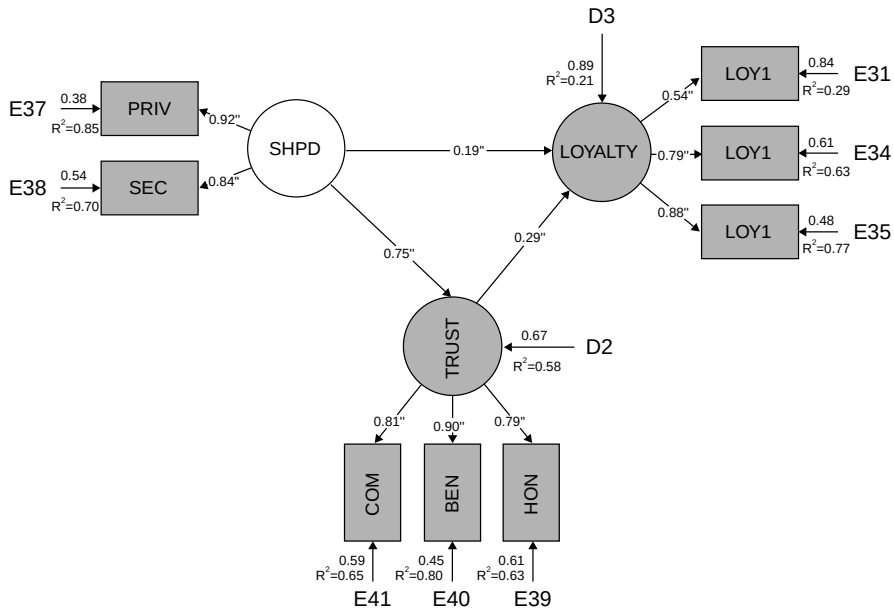

Figure 1.
Structural model. Standardized solution

The results of this research allow to remedy, to a certain extent, the scarcity of empirical studies that have designed and validated measuring scales for the concepts of privacy, security, trust and loyalty on the internet, as well as testing the relationships between them. Specifically, in this study, we have seen that an individual's loyalty to a web site is closely linked to the levels of trust. Thus, the development of trust not only affects the intention to buy, as shown by previous

Indicator	Recommended value	Value
Absolute fit		
χ^2	$p > 0.05$	17.681, 17 gl $p = 0.40922$
Satorra-Bentler χ^2	$p > 0.05$	14.2363; $p = 0.65031$
RMSEA	RMSEA < 0.08	0.011
GFI	Close to 1	0.988
Incremental fit		
NFI	NFI > 0.9	0.989
NNFI	NNFI > 0.9	0.999
AGFI	Close to 1	0.975
CFI	Close to 1	1
RCFI	Close to 1	1
IFI	Close to 1	1
Parsimony fit		
Normed χ^2	(1; 5)	1.046

Table IV.
Structural model fit indicators

researchers (Jarvenpaa *et al.*, 2000), but it also directly affects the effective purchasing behavior, in terms of preference, cost and frequency of visits, and therefore, the level of profitability provided by each consumer. In addition, our analyses show that trust in the internet is particularly influenced by the security perceived by consumers regarding the handling of their private data by the web site.

7.1 Implications for public sector management and private companies

When we look at the results of this research, we see that there is a logical sequence between the variables (perceived security in private data handling, trust and loyalty). This logical sequence implies that surpassing low levels of trust depends on the proper management of legislative, technical and business measures. In fact they are what, when taken together, determine the levels of security and privacy perceived by the consumer. Such management needs to give priority to increase the security and privacy of communications, as this will in turn increase trust, and in the long run favor the creation of a more faithful market. Because of this, we should analyze in more detail the aspects that might affect the levels of perceived security in private data handling. These aspects may be distinguished in terms of the agents responsible for them, basically the private or public sector.

Traditionally, public sector measures regarding internet privacy, security and trust have followed two lines of action: measures of a legal nature and communication policies.

In relation to the legal measures, we can appreciate that up to now, the measures exercised in the USA and Europe have had no significant effect, because of the lack of resources and the heterogeneous nature of legislation between different countries.

The first cause of this ineffectiveness probably lies in the lack of equilibrium between the regulations' intentions and the resources assigned to them. For example, most developed countries have bodies responsible for overseeing consumer privacy protection (e.g. The Federal Trade Commission, in the USA; The Office of Information Commissioner, in the UK; Der Bundesbeauftragte für den Datenschutz, in Germany; Garante per la Protezione dei dati Personali, in Italy; or Agencia de Protección de Datos, in Spain). These bodies often have insufficient human and technical resources to

monitor the enormous number of internet transactions. They also have to abide by the demanding criteria set by national and international legislation regarding data protection, criteria which obviously call for more ambitious material resources.

The second cause of this ineffectiveness is the heterogeneous nature of legislation between different countries. In the USA, there is a great deal of inconsistency, because while activities such as spamming are harshly prosecuted in some states, in others there is greater tolerance. In European countries, privacy protection is more homogeneous, since it emanates from directives issued for this purpose (e.g. Directive 2002/58/EC of the European Parliament). As well as the differences between the USA and Europe mentioned previously, we have to note the ease with which internet businesses are able to set themselves up in "legal limbos" where it is hard to police them. Thus, it is only through a proper assignation of resources and the standardization of international law with regard to the internet that effective legislative responses may be generated.

Concerning the communication policies, we have to note that measures to be taken by the public sector are not only limited to the passing of regulations. In collaboration with the private sector, there have been various awareness-raising campaigns among internet users (e.g. 1st Worldwide Internet Security Campaign, www.worldwidesecure.org). Up to now, government communication strategies do not appear to have a significant effect. Announcing the appearance of new viruses has a far greater impact than these campaigns. For this reason, more direct measures need to be taken, such as giving users the training they need through free courses in collaboration with the private sector. Indeed, some researchers have shown that more computer-savvy individuals make internet purchases with greater frequency. These practices, carried out in some countries, must of course be accompanied by the consensus of the agents involved, with the appropriate financing.

In the private sector, most of the effort has been put into favoring the self-regulation of the sector. North American industry and, in general, most business organizations at an international level, are not satisfied with the legislation promoted by their governments. This is because new laws have been perceived as being an obstacle to the companies' power to gather a large amount of information from their target segments, and to use it for marketing. This is why various initiatives have appeared to set-up their own body of rules whereby industries with an internet presence can self-regulate their practices (e.g. Electronic Privacy Information Center, www.epic.org/; Electronic Frontier Foundation, www.eff.org/; BBBonline, www.bbbonline.org). Most of these self-regulation initiatives have appeared in the USA. In Europe or Asia, this type of action has failed, and thus it seems that legislation and user training is more recommendable in these regions.

In addition, the private and public sectors have responded to user demand by designing various IT applications to ensure security in e-mails, coding or anonymous surfing, among other issues. Prime examples of these technologies are the platform for privacy preferences project (P3P), backed by the World Wide Web Consortium (W3C), the Secure Sockets Layer coding protocol or the public key systems (e.g. PGP) and the electronic signature. However, all these technologies should be publicized in the private sector for them to be applied, and among consumers, so that they can see their usefulness, and in some cases make personal use of them (e.g. digital certificates, firewalls, antivirus programs).

7.2 Future research lines

If we take as our reference point the conclusions and the conceptual and empirical framework of this paper, various future research lines come out. First, it is essential to define whether the conclusions obtained in this research may differ in terms of the category of product analyzed, given that the risk consumers associate with internet purchasing depends on the type of product. Thus, the level of risk associated with financial transactions or paying taxes is substantially greater than that perceived in the purchasing of small household appliances or the reservation of train tickets. Therefore, the need for high levels of trust is probably greater with certain products.

Second, it would be worthwhile analyzing the influence of security as perceived by consumers with regard to the handling of their personal data on the quality of the relationship. This construct is of indubitable interest, since as well as trust, it includes levels of satisfaction (Crosby *et al.*, 1990) and consumer emotional commitment (Roberts *et al.*, 2003), and this would go a long way to helping to predict loyalty to a web site.

Finally, it is worth mentioning the potential influence of new wireless equipment for internet access, Wi-Fi and Wi-Max technology. The Wi-Fi and Wi-Max technologies provide wireless internet access, removing the need for physical connections. This enables the market to be extended to areas without the conventional telephone or cable networks. Although these new technologies are set to generate new business opportunities, they also represent a particular challenge to consumer trust. We need to know how these new technologies and access devices are perceived, in order to see to what extent trust might be an obstacle to the growth of what is known as m-commerce. Specifically, we need to determine whether consumer concern for the security of personal data is similar to that detected in the traditional internet environment and, if necessary, devise the right measures to overcome these barriers.

References

AECE (2005), *Estudio Sobre Comercio Electrónico B2C 2004*, Asociación Española de Comercio Electrónico AECE-FECEMD, available at: www.aece.org (accessed March).

AIMC (2005), *Navegantes en la Red. 7ª Encuesta AIMC a Usuarios de Internet*, Asociación para la Investigación de Medios de Comunicación, available at: www.aimc.es (accessed March).

Anderson, J.C. and Gerbing, D.W. (1988), "Structural equation modelling in practice: a review and recommended two-step approach", *Psychological Bulletin*, Vol. 103, pp. 411-23.

Assael, H. (1992), *Consumer Behaviour and Marketing Action*, PWS-Kent, Boston, MA.

Bagozzi, R. (1994), "Structural equation model in marketing research: basic principles", *Basic Principles of Marketing Research*, Blackwell, Oxford.

Bagozzi, R. and Yi, Y. (1988), "On the evaluation of structural equation models", *Journal of the Academy of Marketing Science*, Vol. 16 No. 1, pp. 74-94.

Bitting, E. and Ghorbani, A. (2004), "Protecting e-commerce agents from defamation", *Electronic Commerce Research and Applications*, Vol. 3, pp. 21-38.

Cheung, C.M.K. and Lee, M.K.O. (2001), "Trust in internet shopping: instrument development and validation through classical and modern approaches", *Journal of Global Information Management*, Vol. 9 No. 3, pp. 23-35.

Chircu, A., Davis, G. and Kauffman, R. (2000), "Trust, expertise, and e-commerce intermediary adoption", paper presented at the Americas Conference on Information Systems.

Chou, D., Yen, D., Lin, B. and Hong-Lam Cheng, P. (1999), "Cyberspace security management", *Industrial Management & Data Systems*, Vol. 99 No. 8, pp. 353-61.

CIB (2003), *Profile of the Internet Shopper. Study of Consumer Internet Barometer*, CIB, available at: www.conference-board.org/pdf_free/CIBpp.ppt

Consumers Union (2002), *A Matter of Trust: What Users Want from Web Sites. Results of a National Survey of Internet Users for Consumer WebWatch*, Consumers Union, San Francisco, CA, available at: www.consumerwebwatch.org/news/report1.pdf

Coulter, K. and Coulter, R. (2002), "Determinants of trust in a service provider: the moderating role of length of relationship", *Journal of Services Marketing*, Vol. 16 No. 1, pp. 35-50.

Crosby, L.A., Evans, K.R. and Cowles, D. (1990), "Relationship quality in services selling: an interpersonal influence perspective", *Journal of Marketing*, Vol. 54, pp. 68-81.

Doney, P. and Cannon, J. (1997), "An examination of the nature of trust in the buyer-seller relationship", *Journal of Marketing*, Vol. 51, pp. 35-51.

Dong-Her, S., Hsiu-Sen, C., Chun-Yuan, C. and Lin, B. (2004), "Internet security: malicious e-mails detection and protection", *Industrial Management & Data Systems*, Vol. 104 No. 7, pp. 613-23.

Donthu, N. and Garcia, A. (1999), "The internet shopper", *Journal of Advertising Research*, Vol. 39 No. 3, pp. 52-8.

Emarketer (2004), "Online consumers continue to worry", available at: www.emarketer.com/Article.aspx?1002913

European Commission (2002), *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, European Commission.

European Commission (2004), *Issues relating to Business and Consumer E-commerce*, Special Eurobarometer 60.0/ Wave 201, European Opinion Research Group.

Flavián, C. and Lozano, F.J. (2003), "Diseño de una escala para medir la orientación al entorno de la nueva formación profesional", *Cuadernos de Economía y Dirección de la Empresa*, Vol. 15, pp. 333-63.

Flavián, C., Martinez, E. and Polo, Y. (2001), "Loyalty to grocery stores in the Spanish market of the 1990's", *Journal of Retailing and Consumer Services*, Vol. 8 No. 2, pp. 85-93.

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

Forrester Research (2001), *Internet Usage & Behaviour: Internet User Study – UK*, December, Forrester Research, Cambridge, MA.

Fung, R. and Lee, M. (1999), "EC-trust (trust in electronic commerce): exploring the antecedent factors", paper presented at the Americas Conference on Information Systems.

Furnell, S.M. and Karweni, T. (1999), "Security implications of electronic commerce: a survey of consumers and business", *Electronic Networking Applications and Policy*, Vol. 9 No. 5, pp. 372-82.

Galanxhi-Janaqi, H. and Fui-Hoon Nah, F. (2004), "U-commerce: emerging trends and research issues", *Industrial Management & Data Systems*, Vol. 104 No. 9, pp. 744-55.

Ganesan, S. (1994), "Determinants of long-term orientation in buyer-seller relationship", *Journal of Marketing*, Vol. 58, pp. 1-19.

Gavish, B. and Gerdes, J.H. (1998), "Anonymous mechanisms in group decision support systems communication", *Decision Support Systems*, Vol. 23, pp. 297-328.

Gefen, D. (2000), "E-commerce: the role of familiarity and trust", *OMEGA: The International Journal of Management Science*, Vol. 28, pp. 725-37.

Gefen, D., Karahanna, E. and Straub, D.W. (2003), "Trust and TAM in online shopping: an integrated model", *MIS Quarterly*, Vol. 27 No. 1.

Goldman, A. (1978), "The shopping style explanation for store loyalty", *Journal of Retailing*, Vol. 53, pp. 33-46.

Gunasekaran, A. and Love, P.D. (1999), "Current and future applications of multimedia technology in business", *International Journal of Information Management*, Vol. 19 No. 2, pp. 105-20.

Gundlach, G. and Murphy, P.E. (1993), "Ethical and legal foundations of relational marketing exchanges", *Journal of Marketing*, Vol. 57, pp. 35-46.

Hair, J.F. Jr, Anderson, R.E., Tatham, R.L. and Black, W.C. (1998), *Multivariate Data Analysis*, Prentice-Hall, Englewood Cliffs, NJ.

Harris Interactive (2002), *Privacy On and Off the Internet: What Consumers Want*, available at: www.aicpa.org/download/webtrust/priv_rpt_21mar02.pdf

Hedelin, L. and Allwood, C. (2002), "IT and strategic decision making", *Industrial Management & Data Systems*, Vol. 102 No. 3, pp. 125-39.

Hildebrant, L. (1987), "Consumer retail satisfaction in rural areas: a reanalysis of survey data", *Journal of Economic Psychology*, Vol. 8, pp. 19-42.

Hoffman, D.L., Novak, T.P. and Peralta, M. (1998), "Building consumer trust online", *Communications of the ACM*, Vol. 42 No. 4, pp. 80-5.

Janda, S., Trocchia, P. and Gwinner, K. (2002), "Consumer perceptions of internet retail service quality", *International Journal of Service Industry Management*, Vol. 13 No. 5, pp. 412-31.

Jarvenpaa, S., Tractinsky, N. and Vitale, M. (2000), "Consumer trust in an internet store", *Information Technology and Management*, Vol. 1 Nos 1/2, pp. 45-71.

Jones, S., Wilikens, M., Morris, P. and Masera, M. (2000), "Trust requirements in e-business", *Communications of the ACM*, Vol. 43 No. 2, pp. 81-7.

Jöreskog, K.G. (1971), "Statistical analysis of sets of congeneric tests", *Psychometrika*, Vol. 36, pp. 109-33.

Jöreskog, K.G. and Sörbom, D. (1993), *LISREL 8: Structural Equation Modeling with the SIMPLIS Command Language*, Scientific Software International, Chicago, IL.

Kelly, E.P. and Erickson, E.G. (2005), "RFID tags: commercial applications v. privacy rights", *Industrial Management & Data Systems*, Vol. 105 No. 6, pp. 703-13.

Kelly, E.P. and Erickson, G.S. (2004), "Legal and privacy issues surrounding customer databases and e-merchant bankruptcies: reflections on Toysmart.com", *Industrial Management & Data Systems*, Vol. 104 No. 3, pp. 209-17.

Kolsaker, A. and Payne, C. (2002), "Engendering trust in e-commerce: a study of gender-based concerns", *Marketing Intelligence & Planning*, Vol. 20 No. 4, pp. 206-14.

Koufaris, M. and Hampton-Sousa, W. (2002), "Customer trust online. Examining the role of the experience with the web site", CIS working papers series, available at: http://cisnet.baruch.cuny.edu/papers/cis200205.htm

Kruck, S.E., Gottovi, D., Moghadami, F., Broom, R. and Forcht, K.A. (2002), "Protecting personal privacy on the internet", *Information Management & Computer Security*, Vol. 10 No. 2, pp. 77-84.

Kumar, N., Scheer, L.K. and Steenkamp, J-B.E.M. (1995), "The effects of supplier fairness on vulnerable resellers", *Journal of Marketing Research*, Vol. 32 No. 1, pp. 42-53.

Lardner, J. (1999), "I know what you did last summer and fall", *US News & World Report*, Vol. 126 No. 15, p. 55.

Larzelere, R.E. and Huston, T.L. (1980), "The dyadic trust scale: toward understanding interpersonal trust in close relationships", *Journal of Marriage and the Family*, August, pp. 595-604.

Lee, J., Kim, J. and Moon, J. (2000), "What makes internet users visit cyber stores again? Key design factors for customer loyalty", *Proceedings of the Conference on Human Factors in Computing Systems CHI 2000*, ACM, New York, NY, pp. 305-12.

Lee, M. and Turban, E. (2001), "Trust in B-to-C electronic commerce: a proposed research model and its application", *International Journal of Electronic Commerce*, Vol. 6 No. 1, pp. 75-91.

Lozano, J. (2002), "La orientación al mercado el contexto universitario español un análisis de sus antecedentes, moderadores y consecuencias", doctoral thesis, University of Zaragoza, Zaragoza.

Lyman, J. (2003), "Symantec report puts corporations, consumers in crosshairs", *Technewsworld*, available at: http://www.technewsworld.com/perl/story/33142.html (accessed March 31).

Mayer, R., Davis, J. and Shoorman, F. (1995), "An integrative model of organizational trust", *Academy of Management Review*, Vol. 20 No. 3, pp. 709-34.

Nilsson, O. and Olsen, J. (1995), "Measuring consumer retail store loyalty", *European Advances in Consumer Research*, Vol. 2, pp. 289-97.

O'Cass, A. and Fenech, T. (2003), "Webretailing adoption: exploring the nature of internet users web retailing behaviour", *Journal of Retailing and Consumer Services*, Vol. 10, pp. 81-94.

Quelch, J. and Klein, L. (1996), "The internet and international marketing", *Sloan Management Review*, March, pp. 60-75.

Ranganathan, C. and Ganapathy, S. (2002), "Key dimensions of B2C websites", *Information & Management*, Vol. 39, pp. 457-65.

Roberts, K., Varki, S. and Brodie, R. (2003), "Measuring the quality of relationships in consumer services: an empirical study", *European Journal of Marketing*, Vol. 37 Nos 1/2, pp. 169-96.

Rowley, J. and Dawes, J. (2000), "Disloyalty: a closer look at non-loyals", *Journal of Consumer Marketing*, Vol. 17 No. 6, pp. 538-49.

Roy, M., Dewit, O. and Aubert, B. (2001), "The impact of interface usability on trust in web retailers", *Internet Research: Electronic Networking Applications and Policy*, Vol. 11 No. 5, pp. 388-98.

Sahay, B. (2003), "Understanding trust in supply chain relationships", *Industrial Management & Data Systems*, Vol. 103 No. 8, pp. 553-63.

Sako, M. and Helper, S. (1997), "Determinants of trust in supplier relations: evidence from the automotive industry in Japan and the United States", *Journal of Economic Behaviour & Organization*, Vol. 34 No. 3, pp. 387-417.

Sanzo, M., Santos, M., Vázquez, R. and Álvarez, L. (2003), "The effect of market orientation on buyer-seller relationship satisfaction", *Industrial Marketing Management*, Vol. 32 No. 4, pp. 327-45.

Siguaw, J., Simpson, P. and Baker, T. (1998), "Effects of supplier market orientation on distributor market orientation and the channel relationship: the distributor perspective", *Journal of Marketing*, Vol. 62, pp. 99-111.

So, M. and Sculli, D. (2002), "The role of trust, quality, value and risk in conducting e-business", *Industrial Management & Data Systems*, Vol. 102 No. 9, pp. 503-12.

So, W.C.M., Wong, T.N.D. and Sculli, D. (2005), "Factors affecting intentions to purchase via the internet", *Industrial Management & Data Systems*, Vol. 105 No. 9, pp. 1225-44.

Sirdeshmukh, D., Singh, J. and Sabol, B. (2002), "Consumer trust, value, and loyalty in relational exchanges", *Journal of Marketing*, Vol. 66, pp. 15-37.

Steenkamp, J.B. and Van Trijp, H.C.M. (1991), "The use of LISREL in validating marketing constructs", *International Journal of Research in Marketing*, Vol. 8, pp. 283-99.

Suh, B. and Han, I. (2003), "The impact of customer trust and perception of security control on the acceptance of electronic commerce", *International Journal of Electronic Commerce*, Spring, pp. 135-61.

Taylor Nelson Sofres Interactive (2002), *Global Ecommerce Report 2002*, available at: www.tnsinfo.com/common/corporate/images/tns/GER2002FullReport.zip

Truste (2003), "Identity theft and spam will deter online shopping this holiday season", press release of Trust 2003, available www.truste.org/about/press_release/12_01_03.php (accessed December 1).

Udo, G. (2001), "Privacy and security concerns as major barriers for e-commerce: a survey study", *Information Management & Computer Security*, Vol. 9 No. 4, pp. 165-74.

van der Smagt, T. (2000), "Enhancing virtual teams: social relations v. communication technology", *Industrial Management & Data Systems*, Vol. 100 No. 4, pp. 148-56.

Wang, H., Lee, M. and Wang, C. (1998), "Consumer privacy concerns about internet marketing", *Communications of the ACM*, Vol. 41, pp. 63-70.

Westin, A.F. (1967), *Privacy and Freedom*, Atheneum, New York, NY.

Wu, J. and Chang, Y. (2005), "Towards understanding members' interactivity, trust, and flow in online travel community", *Industrial Management & Data Systems*, Vol. 105 No. 7, pp. 937-54.

Yoon, S. and Kim, J. (2000), "An empirical validation of a loyalty model based on expectation disconfirmation", *Journal of Consumer Marketing*, Vol. 2, pp. 120-6.

Yousafzai, S.Y., Pallister, J.G. and Foxall, G.R. (2003), "A proposed model of e-trust for electronic banking", *Technovation*, Vol. 23, pp. 847-60.

Further reading

Anderson, E. and Weitz, B. (1989), "The use of pledges to build and sustain commitment in distribution channels", *Journal of Marketing Research*, Vol. 29, pp. 18-34.

Bhattacherjee, A. (2002), "Individual trust in online firm: scale development and initial test", *Journal of Management Information Systems*, Vol. 19 No. 1, pp. 211-41.

Churchill, G.A. (1979), "A paradigm for developing better measures of marketing constructs", *Journal of Marketing Research*, Vol. 16, pp. 64-73.

Ferraro, A. (1998), "Electronic commerce: the issues and challenges to creating trust and a positive image in consumer wide web", *First Monday*, available at: www.firstmonday.dk/issues/issue3_6/ferraro/index.html

Khare, R. and Rifkin, A. (1998), "Trust management on the world wide web", *First Monday*, available at: http://firstmonday.org/issues/issue3_6/khare/index.html

Liebermann, Y. and Stashevsky, S. (2002), "Perceived risks as barriers to internet and e-commerce usage", *Qualitative Market Research: An International Journal*, Vol. 5 No. 4, pp. 291-300.

Moghe, V. (2003), "Privacy management – a new era in the Australian business environment", *Information Management & Computer Security*, Vol. 11 No. 2, pp. 60-6.

Nunnally, J.C. (1978), *Psychometric Theory*, McGraw-Hill, New York, NY.

Nurosis, M.J. (1993), *SPSS. Statistical Data Analysis*, SPSS Inc., Chicago, IL.

Pavlou, P. (2002), "Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model", *International Journal of Electronic Commerce*, Vol. 7 No. 3, pp. 101-34.

Tan, S. (1999), "Strategies for reducing customer's risk aversion and internet shopping", *Journal of Consumer Marketing*, Vol. 16 No. 2, pp. 163-80.

The Conference Board (2004), "Consumers going online before going on the road", press release of Consumer Internet Barometer 2004, available at: www.conference-board.org/economics/consumerBarometer.cfm (accessed June 28).

Appendix. Measurement scales

		Adapted from/new item
Scale for measuring web site user trust		
HON1	I think that this web site usually fulfils the commitments it assumes	Kumar *et al.* (1995)
HON2	I think that the information offered by this site is sincere and honest	Kumar *et al.* (1995)
HON3	I think I can have confidence in the promises that this web site makes	Kumar *et al.* (1995)
HON4	This web site does not make false statements	Kumar *et al.* (1995)
HON5	This web site is characterized by the frankness and clarity of the services that it offers to the consumer	Siguaw *et al.* (1998)
BEN1	I think that the advice and recommendations given on this web site are made in search of mutual benefit	Kumar *et al.* (1995)
BEN2	I think that this web site is concerned with the present and future interests of its users	Kumar *et al.* (1995)
BEN3	I think that this web site takes into account the repercussions that their actions could have on the consumer	Kumar *et al.* (1995)
BEN4	I think that this web site would not do anything intentional that would prejudice the user	Kumar *et al.* (1995)
BEN5	I think that the design and commercial offer of this web site take into account the desires and needs of its users	Roy *et al.* (2001)
BEN6	I think that this web site is receptive to the needs of its users	Roy *et al.* (2001)
COM1	I think that this web site has the necessary abilities to carry out its work	Roy *et al.* (2001)
COM2	I think that this web site has sufficient experience in the marketing of the products and services that it offers	Roy *et al.* (2001)
COM3	I think that this web site has the necessary resources to successfully carry out its activities	Roy *et al.* (2001)
COM4	I think that this web site knows its users well enough to offer them products and services adapted to their needs	Roy *et al.* (2001)
Scale for measuring privacy		
PRIV1	I think this web site shows concern for the privacy of its users	Janda *et al.* (2002)
PRIV2	I feel safe when I send personal information to this web site	O'Cass and Fenech (2003)

(*continued*)

Table AI.

		Adapted from/new item
PRIV3	I think this web site abides by personal data protection laws	New item
PRIV4	I think this web site only collects user personal data that are necessary for its activity	New item
PRIV5	I think this web site respects the user's rights when obtaining personal information	New item
PRIV6	I think that this web site will not provide my personal information to other companies without my consent	Cheung and Lee (2001)
PRIV7	This web site does not send e-mail advertising without the user's consent	New item
Scale for measuring security		
SEC1	I think this web site has mechanisms to ensure the safe transmission of its users' information	Ranganathan and Ganapathy (2002)
SEC2	I think this web site shows great concern for the security of any transactions	Ranganathan and Ganapathy (2002)
SEC3	I think this web site has sufficient technical capacity to ensure that no other organization will supplant its identity on the internet	O'Cass and Fenech (2003)
SEC4	I am sure of the identity of this web site when I establish contact via the internet	O'Cass and Fenech (2003)
SEC5	When I send data to this web site, I am sure that they will not be intercepted by unauthorized third parties	New item
SEC6	I think this web site has sufficient technical capacity to ensure that the data I send will not be intercepted by hackers	New item
SEC7	When I send data to this web site, I am sure they cannot be modified by a third party	New item
SEC8	I think this web site has sufficient technical capacity to ensure that the data I send cannot be modified by a third party	New item
Scale for measuring loyalty		
LOY1	I visit this web site more frequently than others of the same category	New item
LOY2	This is the web site where I purchase the majority of the products and services in this internet category	New item
LOY3	This is my favorite site for purchasing the products and services in this internet category	New item

Table AI.

Corresponding author
Carlos Flavián can be contacted at: cflavian@unizar.es