The Effect of Consumer Privacy Empowerment on Trust and Privacy Concerns in E-Commerce

THOMAS P. VAN DYKE, VISHAL MIDHA AND HAMID NEMATI

A b s t r a c t

Privacy concerns and a lack of trust have been shown to reduce consumer's willingness to transact with an online vendor. Understandably, firms are searching for methods to reduce consumer privacy concerns and increase trust. In this study, we introduce a new construct – consumer privacy empowerment. We then propose and test a theoretical model that examines the relationship between consumer privacy empowerment, familiarity, privacy concern and trust. Results indicate support for the model and suggest that perceived privacy empowerment has a strong influence on both privacy concern and trust in e-commerce.

Keywords: Electronic commerce, privacy, trust, empowerment

INRODUCTION

> Some online sellers are hiring prominent auditors to verify their privacy policies and increase trust (Headline *The New York Times*, 18 September 2000)
>
> According to Suzi LeVine, Expedia's marketing manager: 'This won't directly increase sales, but it will increase customer confidence in the site. And that, combined with all the services we provide, will increase sales.' (Tedeschi 2000)

The above quote provides anecdotal evidence that executives at e-commerce firms believe that there are links between the consumer's perception of online privacy, trust in the site and increased sales. The quote is indicative of the efforts that online firms have been making to 'break through the wall of mistrust that separates them from millions of would-be shoppers who fret about online privacy' (Tedeschi 2000).

Westin (1967) defined the right to privacy as 'the right of the individuals … to determine for themselves when, how, and to what extent information about them is communicated to others'. Information privacy has been described as the claim that individually identifiable information not be generally available to other individuals or organizations, and in cases where that data are possessed by another party, the individual must be able to exercise a substantial degree of control over the information and its use (Clarke 1999). Both of these definitions emphasize the importance of individual control over personal information as central to the concept of privacy.

The concept of control is also the basis of three of the Federal Trade Commission's (FTC) Fair Information Practices that serve as guidelines for the collection of information online (e.g., notice, choice and access) (Sheehan and Hoy 1998). These fair information practices are the basis of an effort at self-regulation in the online industry over matters of information collection and use.

The findings of Olivero and Lunt (2004) suggest that when faced with an increase in awareness of privacy threats, consumers tend to reduce trust and demand more control. This suggests that firms who delegate that control to the consumer may be able to gain a competitive advantage. Without any currently effective legislation restricting the collection and use of information online in the United States,

A u t h o r s

Thomas P. Van Dyke
(tpvandyk@uncg.edu) is an Assistant Professor of Information Systems and Operations Management at the University of North Carolina, Greensboro.
Vishal Midha
(v_midha@uncg.edu) is a doctoral student at University of North Carolina, Greensboro.
Hamid Nemati
(nemati@uncg.edu) is an Associate Professor of Information Systems and Operations Management at the University of North Carolina, Greensboro.

Copyright © 2007 Electronic Markets
Volume 17 (1): 68–81. www.electronicmarkets.org DOI: 10.1080/10196780601136997

companies have wide latitude concerning the particulars of their privacy policies and more specifically the amount to which they are willing to empower consumers by ceding to them control over their personally identifiable information. This research seeks to investigate the efficacy of that strategy.

In this paper, we introduce a new construct – consumer privacy empowerment, and report the results of a study that examines the relationship between consumer privacy empowerment, familiarity, privacy concern and trust in an e-commerce environment.

THEORETICAL DEVELOPMENT OF RESEARCH MODEL

A conceptual model of all four constructs of interest in this study and their proposed relationships is shown in Figure 1.

Consumer trust

Trust can be defined as the willingness to make oneself vulnerable to actions taken by the trusted party based on the feeling of confidence or assurance (Gefen 2002). Trust is complex, multidimensional and context specific. (See McKnight and Chervany (2002), for a typology of trust in e-commerce.) Lee and Turban (2001) proposed a model of 'consumer trust in Internet shopping' that included trust in the merchant and trust in the Internet shopping medium along with contextual factors such as the effectiveness of the security infrastructure. Tan and Thoen (2001) proposed a generic model of trust for electronic commerce that likewise identifies 'transaction trust' as being dependent on both trust in the other party and trust in control mechanisms. Party trust is equivalent to trust in the Internet merchant and control trust includes trust in the procedures, rules and protocols that monitor and control the performance of the transaction. Tan and Thoen suggest that control trust can be a substitute for party trust when attempting to create a level of transaction trust necessary to encourage participation in an e-commerce transaction. It is generally agreed that some level of trust is required in order for people to engage in e-commerce transaction. The development of trust between businesses and consumers is seen as crucial to the expansion of e-commerce markets (Hoffman *et al.* 1999).

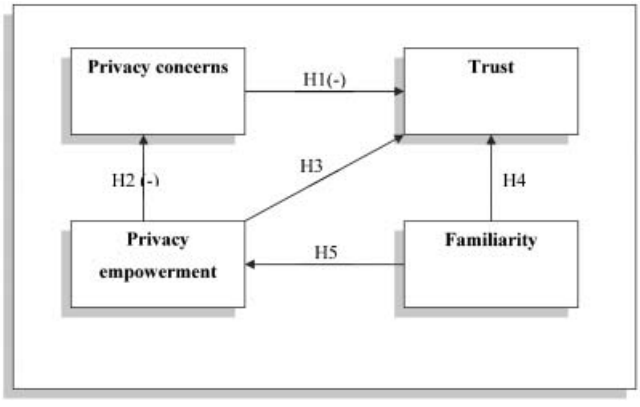

Figure 1. Conceptual model

So and Sculli (2002) provide a comprehensive review of the many advantageous effects of customer trust on general business related behaviour including: a reduction in transaction complexity (Sheth and Pravatiyar 2000); a reduction in transaction costs (Fukuyama 1995, Hart and Johnson 1999); the development of long-term relationships with customers that are important elements in long-term profits (Hart and Johnson 1999, Gefen 2000); a reduction in the level of concern for the confidential information sharing that is necessary for business transactions (Hart and Johnson 1999); and a reduction of perceived risk (Jarvenpaa *et al.* 2000). Trust also reduces the need for comprehensive legislation and enforced regulation (Fukuyama 1995).

In addition to its benefits for business in general, trust has been shown to have special importance in the e-commerce environment. For example, trust is a critical factor in stimulating purchases over the Internet (Quelch and Klien 1996). Although traditionally trust has been defined in interpersonal terms, when sales-people are absent from the purchase transaction, as in Internet shopping, then the primary focus of the customer's trust is on the firm itself (Chow and Holden 1997). In an e-commerce context, trust in an Internet retailer has been shown to reduce the perceived risk associated with purchasing from that retailer (Jarvenpaa *et al.* 2000). Also important in the context of e-commerce is the fact that studies have shown that customer trust is a significant antecedent of a customer's willingness to transact business with an online vendor (Gefen 2000, Jarvenpaa *et al.* 2000, Liu *et al.* 2004). In addition, trust has also been shown to effect consumer's intention to re-visit the site and recommend the site to others (Liu *et al.* 2004). Trust creates in consumers a willingness to engage in transactions that expose a person to risk without the ability to control the behaviour of the other participants. This effect makes trust an important antecedent of e-commerce success (McKnight and Chervany 2002). It is clear that many consumers do not trust companies to keep their personal information private and they do not trust Internet technology to secure their financial transactions (Hart and Johnson 1999). This lack of trust is costing e-retailers billions in lost sales. As an article in the *Wall Street Journal* put it ''It seems that trust equals revenue, even online' (Petersen 2001).

In order to gain consumer trust, e-commerce firms must find a way to convince consumers that the personal information obtained through their websites will remain secure. Web merchants have employed a wide variety of

approaches to increase consumer trust. These methods include secure, encrypted communication, third party payers (e.g., Paypal) published privacy policies, and third party certifications such as TRUSTe, WebTrust and BBBOnline. Retailers realize that it is trust that must be created in order to counter the effects of privacy and security concerns.

Given the importance of trust in the e-commerce environment, the factors that produce a perception of trustworthiness within consumers need to be identified. Their interactions need to be understood, and their relative importance determined. Understanding the roles of these different factors would allow online retailers to ease consumers' concerns, and could improve customer perceptions of web retailing.

Familiarity

'Familiarity is an understanding, often based on previous interactions, experiences and learning, of what, why, when and where others do what they do' (Gefen 2000: 727). Familiarity can be seen as an antecedent to trust. Blau (1964) contends that trust is developed through previous interactions with the trusted party. Previous interactions lead to an acquaintance (i.e., familiarity) with the other party and provide information about its trustworthiness and what to expect of its behaviour. Familiarity helps one set realistic expectations of the future behaviour of the trusted party.

In this way familiarity with an e-commerce vendor reduces social uncertainty. When making an e-commerce transaction, the consumer is faced with a very complex array of possible risks and behaviours on the part of the vendor, some of which could be harmful to the consumer. Familiarity with the firm and the website provides the user with context and helps them to anticipate the vendor's behaviour and ground their expectations in experience (Gefen and Straub 2003).

Gefen (2000) investigated the relationship between familiarity and trust in e-commerce. His results indicated that familiarity positively affected trust and that both trust and familiarity had a positive effect on purchase intentions in an e-commerce setting. He cites the contention put forth by Blau (1964) that familiarity and trust are both beneficial to e-commerce because they work to reduce the social complexity of the e-commerce transaction.

When familiarity is lacking, party trust (i.e., trust in the firm) is de-emphasized and control trust (i.e., trust in rules, regulations and policies) becomes more important. For example Grewal *et al.* (2003) reported that published privacy policy statements were more beneficial for Web merchants that lacked name recognition than for those with a more established reputation. Utilizing slightly different terms, a study by Schoder and Haenlein (2004) demonstrated that control trust, which they referred to as institutional trust, was significantly more important to the seller than relational trust, based on experience over time or calculative trust, based on risk–reward calculations.

Prior experience can be a basis for trust. Familiarity can create trust when those experiences are favourable or ruin trust when they are unfavourable. Assuming that the majority of e-commerce firms perform in an ethical manner and do not violate the privacy rights of their customers, experience with those e-vendors should lead to an increase in trust. In a study of e-consumer behaviour, Hong-Youl and Perks (2005) found that brand familiarity was a antecedent of brand trust.

Based on this discussion and previous research finding, we propose the following hypothesis:

Hypothesis 4: Familiarity positively affects trust

Although undertaken in a different context, the theoretical underpinnings of Ford (2000) suggest implications for the current study. In a paper investigating how the Internet is changing the relationship between consumers and health care providers, Ford (2000) reported that consumers get the perception of empowerment when they have familiarity with the health care issue at hand. Consumers collect information from the Web to familiarize themselves with such issues, which helps them make joint decisions with their physicians, resulting in perceived empowerment. It is logical to assume that some familiarity with a firm's online presence and privacy policies might be required to induce an increased perception of privacy empowerment. This leads to the next hypothesis, which can be stated as:

Hypothesis 5: Familiarity positively affects empowerment

Privacy concerns

In order to compete in a highly competitive global economy, companies rely on large amounts of information to build relationships with current customers and to attract new customers. The marketing strategies of many successful firms increasingly depend on the use of detailed customer information (Bessen 1993, Culnan and Armstrong 1999). Therefore, it is not surprising that companies wish to maintain the right to collect, use and in some cases sell customer information.

There are two potential problems for the firm associated with the ever-increasing collection and use of detailed personal information. First is the potential of precipitating legal restrictions on information collection and use. The other potential problem stems from the fact that the very techniques of information collection and use that provide value to organizations and to their customers also raise privacy concerns among consumers

(Bloom *et al.* 1994, Liao and Cheung 2001). A heightened awareness of information collection on the Web has been shown to result in a decrease in trust (Olivero and Lunt 2004).

Smith *et al.* (1996) suggest several dimensions of concern related to information privacy. *Collection* is a general concern that large amounts of personally identifiable data are being collected and stored. *Unauthorized secondary use (internal)* is the concern that information collected for one purpose could be used for another, unauthorized purpose by the same organization. *Unauthorized secondary use (external)* is the concern that information collected for one purpose could be used for another, unauthorized purpose after disclosure to an external organization. *Improper access* is the concern that personal data are available to people not properly authorized to view the data. *Errors* names the concern that the protections against deliberate or accidental errors are not adequate. One concern that Smith *et al.* listed as tangential to the privacy issue, but which seems relevant in an e-commerce setting is *Combining data*. This is the concern that several seemingly innocuous pieces of information in disparate databases may be combined to create personally identifying information that the user does not wish to disclose.

Like trust, privacy is a complex, multidimensional and context specific construct. It is influenced by factors as heterogeneous as legal and regulatory environments, cultural norms and security technology (Galanxhi and Nah 2006). A complete discussion of factors affecting privacy is beyond the scope of this paper. A more thorough discussion of privacy issues in an environment of ubiquitous commerce along with an integrated privacy framework is presented in Galanxhi and Nah (2006).

It is important to realize that privacy concerns are not merely psychological constructs. There is ample evidence that privacy concerns actually alter consumer behaviour in a number of negative ways. According to a survey by AT Kearny, 52% of respondents reported abandoning an online purchase transaction due to privacy concerns (Ranganathan and Grandon 2002). Total avoidance of online shopping, refusal to provide information and abandoning transactions are not the only responses to privacy concerns. Polls show that 30–40% (Hoffman *et al.* 1999) of Web users provide false information online. Reasons given include the desire to remain anonymous, avoidance of spam email, and concern about how the website will use the information. A consequence of this online lying is that much of the information collected by websites is wrong. This both increases the cost and decreases the value of the data collected (Gellman 2002). The Federal Trade Commission estimates that online retail sales were reduced by up to $18 Billion in 2002 due to concerns over privacy (FTC 2000). The FTC also cited a survey showing that 92% of households with Internet access stated that they do not trust online companies to keep their personal information confidential (FTC 2000). A study by Liu *et al.* (2004) concluded that privacy has a strong influence on whether a consumer trusts an e-vendor. Their results also indicate that trust subsequently influences behavioural intentions to purchase, visit the site again, or recommend the site to others. In order to alleviate privacy concerns and encourage information sharing, companies must increase trust and decrease perceived risk (Culnan and Armstrong 1999). These findings suggest the following hypothesis:

Hypothesis 1: Increased privacy concerns negatively affect trust.

Privacy empowerment

In the business world, the term 'empowerment' has been used most widely in two contexts, employee empowerment and consumer empowerment. Both constructs share in common the idea of shifting power or *control* from higher levels down to the individual. Individual control also plays an important part in the management of privacy (Tavani and Moor 2001). We build upon the literature from consumer empowerment, employee empowerment and the psychological construction of empowerment along with the concept of individual control and its role in privacy to define a new construct – consumer privacy empowerment.

Consumer empowerment concerns shifting the balance of power from service providers, who have traditionally held power, to the consumers who have traditionally been powerless (Hoffman *et al.* 1999). Wathieu *et al.* (2002) suggest that one of the elements that makes a consumer feel ''empowered'' is control of the choice set composition. They argue that ''the perception of empowerment will be driven less by the size of the provided choice set than by the consumer's ability to specify and adjust the choice context. According to this view, the experience of empowerment derives not from more choices, but from one's flexibility in defining one's choices.'' (Wathieu *et al.* 2002: 299). Moreover, a subjective perception of control in choice has been shown to yield positive long-term effects in terms of satisfaction and general happiness (Langer 1983).

From the management and organizational theory perspective, 'empowerment' broadly refers to the process of delegating greater discretion and resources to subordinates: distributing control in order to better serve both customers and the interests of employing organizations. It's a process that builds trust between the employee and the company (Spreitzer 1995).

Thomas and Velthouse (1990) suggested that psychological empowerment is manifested through four

cognitions: meaning, competence, self-determination and impact. *Meaning* is the value of a work goal or purpose, judged in relation to an individual's own standards or ideals. *Competence*, also known as self-efficacy, is an individual's belief in his or her ability to perform activities with skill. *Self-determination* is an individual's perception of having choice in initiating and regulating actions. It reflects autonomy over the conduct of work-related behaviours. *Impact* is the degree to which an individual believes they can influence work outcomes. The perception of impact is not a universal construct, but rather is specific to a particular work context.

These four dimensions are argued to combine additively to create an overall construct of psychological empowerment. Psychological empowerment reflects an orientation in which an individual both wishes and feels able to shape his or her work role and context (Spreitzer 1995). It should be considered a continuous variable. People should be thought of as more or less empowered, rather than empowered or not empowered (Spreitzer 1995).

We see from the above discussion that the delegation of control is the basis of empowerment. Control is also central to the concept of privacy. Westin (1967) defined the right to privacy as 'the right of the individuals … to determine for themselves when, how, and to what extent information about them is communicated to others'. Information privacy has been described as the claim that individually identifiable information not be generally available to other individuals or organizations, and in cases where that data is possessed by another party, the individual must be able to exercise a substantial degree of control over the data and its use (Clarke 1999). According to Fried (1984: 209): 'Privacy is not simply an absence of information about us in the minds of others, rather it is the *control* we have over information about ourselves.' All of these definitions emphasize the importance of individual control over personal information as central to the concept of privacy.

Another indicator of the potential importance of empowerment is the fact that the concept of empowering the individual to control privacy is embedded within three out of four of the FTC's Fair Information Practices (notice, choice and access) (FTC 2000, Sheehan and Hoy 1998). The Fair Information Practices (FIP) serve as guidelines for the collection of information online. They form the basis of an effort at self-regulation in the online industry over matters of information collection and use. These principles were suggested to industry by the FTC in response to increased privacy concerns among consumers. The three that incorporate the concept of improved individual control are:

1. *Notice*: The most fundamental principle is notice. Consumers should be given notice of an entity's information practices including what information they collect, how they collect it (e.g. directly or through non-obvious means such as cookies), how they use it, how they provide choice, access and security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site. This information should be disclosed before any personal information is collected. It is assumed that without notice, a consumer is unable to make an informed decision as to whether and to what extent to disclose personal information. The provision of information is seen as a method to reduce the asymmetries of information between the vendor and the consumer. Information in this context is seen as empowering because once it is provided, the consumer is better able to protect their own interests and make decisions based on informed consent. However, Howells (2005) has warned that information alone is not sufficient to empower consumers. He cites several factors that limit the effectiveness of empowerment by information, the most germane of which is the limited ability of consumers to understand and process information. If the information provided by *notice* cannot be understood by the consumer then any claims of subsequent decisions being based on informed consent are illusory.
2. *Choice*: Consumers should be provided with choices as to how their personal identifying information is used beyond the use for which the information was provided (e.g., to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities). These choices or consents are usually available as either 'opt-in' or 'opt-out'. Wathieu *et al.* (2002) suggest that ability to control results in the consumer's perceived empowerment. This perceived empowerment comes from flexibility in defining one's choices. Hence, by granting the right to control the decision on their personal information, the consumer's perception of empowerment can be increased.
3. *Access*: Websites should offer consumers reasonable access to the information a website has collected about them, including a reasonable opportunity to review the information and to correct inaccuracies. This principle clearly allows a consumer to control personal information and allows one to safeguard against the collection and maintenance of harmful erroneous information (Tavani and Moor 2001). Research conducted for the online banking industry concluded that consumers tend to think about security and privacy in broad terms that include crimes, invasion of privacy and errors. Over time as neither crimes nor serious invasions of privacy are encountered during consumer's lives online, research indicated that their concerns tended to

focus largely on protecting themselves against errors and having recourse to correct any errors that occur (Roboff and Charles 1998). It is clear that providing consumers with the ability to access and amend their personal information is essential in order to reduce the level of privacy concern about errors.

Tavani and Moore (2001) posit that control is essential in the justification and management of privacy. They define three ways in which control helps in the management of privacy as choice, consent and correction. These three constructs are related to the three Fair Information practices previously enumerated. Tavani and Moore's concept of 'choice' is embedded in the FIP called 'Notice' in that it requires informed choice. The information provided by notice is needed to make informed decisions regarding one's personal privacy. 'Consent' is roughly analogous to the FIP named 'Choice' as it includes the opt-in or opt-out options that can be used by the vendor to gain consent. 'Correction' is included in the Access principle. The ability not only to access but also to amend if necessary is the cornerstone of Access.

Olivero and Lunt (2004) performed a qualitative study to determine the effect of perceived privacy risk on the relative roles of trust and control as they relate to the willingness to disclose information in e-commerce. Their results indicate that perceived risk and the awareness of information collection/extraction (i.e., privacy concerns) are associated with a shift in consumer's concerns from issues of trust to issues of control. An increased awareness of privacy risk was found to reduce the level of trust and increase the demand for control among consumers.

A review of the literature has demonstrated that privacy and control are complementary notions that reinforce each other. We have shown that privacy is often defined in terms of control. It has also been documented that consumer control is at the core of the Fair Information Practices recommended by the FTC to reduce privacy and security risks for online consumers. Furthermore, we have documented that increases in privacy concern and decrease in trust result in an increased demand for control. This research is focused on examining the effect of granting that control to the consumer. It is the delegation of control that empowers the individual.

We have integrated these control-related phenomena to define a new construct – *perceived privacy empowerment*. Perceived privacy empowerment is a psychological construct related to the individual's perception of the extent to which they can control the distribution and use of their personally identifying information. We have shown that privacy comes from having control over your personal information and privacy concerns are related to a lack of such control. Privacy empowerment is simply delegating some control over personal information to the consumer. Therefore, we postulate that an increase in the consumer's perception of privacy empowerment will result in a decrease in the level of privacy concern.

Hypothesis 2: Perceived privacy empowerment negatively affects privacy concern.

By combining the effects of Hypotheses 1 and 2, we believe that consumer privacy empowerment may have a positive indirect effect on trust resulting from the lower level of privacy concern. Moreover, it is possible that privacy empowerment may have a direct effect on trust as well. We have identified two possible mechanisms by which empowerment might directly effect trust.

First, recall that overall trust in an e-commerce transaction includes both party trust and control trust and that one type might be substituted for another (Tan and Thoen 2001). Control trust includes trust in the procedures, rules and protocols that monitor and control the performance of the transaction. It is possible that a consumer's knowledge of a firm's policy of consumer privacy empowerment might increase the level of control trust. This control trust can be a substitute for party trust when attempting to create a level of overall transaction trust necessary to encourage participation in an e-commerce transaction.

A second mechanism by which perceived empowerment might affect trust is through market signalling. In a transaction that requires trust, the act of trusting exposes the trusting party to the possibility of a negative outcome. There is a risk associated with the transaction and the consumer will not complete the transaction unless the risk is judged to be acceptably low. The problem for consumers trying to estimate that risk is difficult because they may have limited knowledge about the trustworthiness of the firm. Individual e-commerce retailers may be characterized as either trustworthy or untrustworthy in their handling of private information. Trustworthy retailers can attempt to differentiate themselves by taking actions that are less costly to them than they are to the untrustworthy retailers. These actions serve as signals to the market (Lee *et al.* 2005).

In a different context, product warranties or money back guarantees serve as signals of quality or product reliability (Kirmani and Rao 2000, Price and Dawar 2002). In this case the signal would be the adoption and/or publication of policies that empower the consumer to control their private information. According to signalling theory, this signal should help the consumer resolve the classification problem of determining if the firm is trustworthy or not. If the adoption of privacy empowerment policies works in this way then we would expect that higher levels of perceived privacy empowerment would be associated with increased levels of trust.

Hypothesis 3: Perceived privacy empowerment positively affects trust.

RESEARCH METHODOLOGY

Sample and procedures

In order to test the data collection instrument, a pilot study was conducted utilizing 48 students (both graduate and undergraduate) at a large university in the South Eastern United States. The pilot studies revealed some minor problems with the instrument, which are discussed below. After modifying the instrument based on the responses from the pilot study, we conducted an online survey in order to test the research model. The survey was administered to 287 experienced users. Experienced users were defined as people who had made at least one online purchase. The survey resulted in 220 usable responses.

Measures

Familiarity, privacy concerns and trust were measured using existing instruments. Except for demographic questions, all items were assessed using a 5-point Likert scale with end points of 'strongly disagree' and 'strongly agree'. The instruments for Trust and Familiarity utilized six and three items respectively and were adapted from Gefen and Straub (2003). One item for the trust construct was dropped after it failed to load significantly in factor analysis. The Privacy Concerns construct was operationalized using eleven items from Smith *et al.* (1996).

Perceived privacy empowerment is a new construct. For purposes of this study, we did not attempt any objective measure of actual privacy empowerment. Instead we measured the consumer's perceived privacy empowerment. While it is logical to assume that the two are correlated, the relationship between the actual levels of empowerment and perceived empowerment is beyond the scope of this study. In order to measure perceived privacy empowerment, we created a four-item scale based on the four cognitions of psychological empowerment described by Spreitzer (1995). The four constructs for employee empowerment were Meaning, Self-efficacy, Self-determination and Impact. Four new items were adapted from items used in an instrument designed to measure employee psychological empowerment. The items were modified to fit the context of e-commerce privacy. The perceived consumer privacy empowerment scale included four items related to: (1) their perception that the tools/options provided to them gave them what they needed to control their personal information; (2) degree of autonomy in determining how personal information would be used; (3) their influence on what happened to the information; and (4) the overall perception of empowerment provided by the firm. The reliability and number of items in each scale are shown in Table 1.

Test of constructs

The appropriateness of using factor analysis was determined by using the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and Bartlett's test of sphericity. For the collected data, the KMO is 0.822 and the chi-square statistic is 1899.626 ($p<0.000$), thus indicating that factor analysis is appropriate (Hair *et al.* 1998).

The next step in factor analysis is to perform principle components analysis (PCA). PCA examines the factor loading of each indicator, extracting items that do not significantly load on the construct of interest. An item is extracted if it does not load above 0.60 on its own construct or above 0.40 on another construct.

After determining the appropriate number of factors, the final factor matrix was rotated using Oblique rotation. Oblique rotation was chosen over varimax because it allows factors to correlate to one another and is used when factors are highly correlated as was the case in this study (Hair *et al.* 1998).

Note that the instrument contains a total of seven factors, not four as represented in the model. This is due to the fact that Privacy Concern is comprised of four dimensions or sub-constructs as defined by Smith *et al.* (1996). Items P1–P3 measure collection concern, P4–P5 measure concern for unauthorized access, P6–P8 measure concern for errors, and P9–P11 measure concern for unauthorized secondary use. The other factors represent trust, familiarity and empowerment.

All the factor loadings are greater than 0.6, with the exception of E23. The loading for E23 is very close to 0.6. Item T16 was dropped as its loading value was 0.509. Factor loadings for the remaining items are shown in Table 2.

The measurement model was assessed for convergent and discriminant validity and reliability using statistical formulas and SPSS (Chin 1998, Compeau *et al.* 1999). Convergent and discriminant validity was assessed by applying two criteria: (1) the square root of the average variance extracted (AVE) by a construct from its

Table 1. Scale reliability and number of items

Construct	*Cronbach alpha*	*Number of items*
Privacy Concerns (PC)	0.801	11
Trust (TR)	0.790	5
Familiarity (FM)	0.710	3
Privacy Empowerment (Pem)	0.803	4

Table 2. Pattern matrix

	Component						
	1	*2*	*3*	*4*	*5*	*6*	*7*
P1			0.960				
P2			0.968				
P3			0.888				
P4						0.707	
P5						0.825	
P6				0.920			
P7				0.832			
P8				0.940			
P9					0.614		
P10					0.856		
P11					0.875		
T12	0.690						
T13	0.801						
T14	0.652						
T15	0.802						
T17	0.879						
F18		0.803					
F19		0.806					
F20		0.872					
E22							0.692
E23							0.597
E24							0.800
E25							0.734

indicators should be at least 0.707 (i.e., AVE>0.50) and exceed correlations with other constructs (Chin 1998, Hair *et al.* 1998); and (2) standardized item loadings should be at least 0.707 (Agarwal and Karahanna 2000, Compeau *et al.* 1999). Table 3 contains the loadings for each item. The square root of the AVE for each construct is located on the diagonal of the table and is shaded. As shown in the table, both criteria (1) and (2) are satisfied, therefore, convergent and discriminant validity are supported.

Two measures of reliability for the seven constructs were determined using Cronbach's alpha and Composite Reliability (CREL) (Chin 1998). Composite reliabilities (similar to Cronbach's alpha) of 0.70 or higher are considered adequate (Compeau *et al.* 1999). CREL is considered more robust than Cronbach's alpha because it weighs items differently depending on factor loading considerations (Agarwal and Karahanna 2000). Looking at Table 3, both CREL and Cronbach's alpha were greater than 0.70, indicating high reliability.

RESEARCH RESULTS

Demographics

We collected 220 usable responses from experienced online shoppers. Respondents ranged in age from 20 to 47 with an average age of 23. The respondents were fairly evenly distributed by gender with 120 males (55%) and 100 females (44%). The average Internet usage per week for the sample was 9.02 hours.

Measurement models

Figure 2 displays the structure and estimated parameters of second order factor model for privacy concerns. All the loadings are significant, which provide evidence to support convergent validity of the measured items (Anderson and Gerbing 1988). The overall model fit is significant (chi-sq value=53.96, df=40, p=0.0695, RMSEA=0.040, GFI=0.96, AGFI=0.93, CFI=0.98, NFI=0.95). The second order model suggests that privacy has four different dimensions that are part of a single underlying construct, namely, consumers' privacy concerns. All the results for first as well as second order

Table 3. Reliability and average variance extracted

Construct	*Cronbach's Alpha*	*CREL*	*AVE*	*PC1*	*PC2*	*PC3*	*PC4*	*TR*	*FM*	*CEm*
PC1	0.818	0.957	0.882	0.939						
PC2	0.707	0.741	0.590	0.152	0.768					
PC3	0.800	0.926	0.808	0.326	0.143	0.899				
PC4	0.660	0.831	0.626	0.078	0.014	0.223	0.791			
TR	0.790	0.877	0.592	−0.394	−0.251	−0.351	−0.288	0.769		
FM	0.710	0.867	0.685	−0.025	0.112	−0.134	−0.034	0.270	0.828	
CEm	0.803	0.801	0.503	−0.443	−0.279	−0.390	−0.280	0.522	0.274	0.709

Notes: CREL: Composite Reliability; AVE: Average Variance Extracted. Diagonal Elements (shaded) are the square root of the variance shared between the constructs and their measurement (AVE). Off diagonal elements are the correlations among constructs. Diagonal elements should be larger than off-diagonal elements in order to demonstrate discriminant validity.

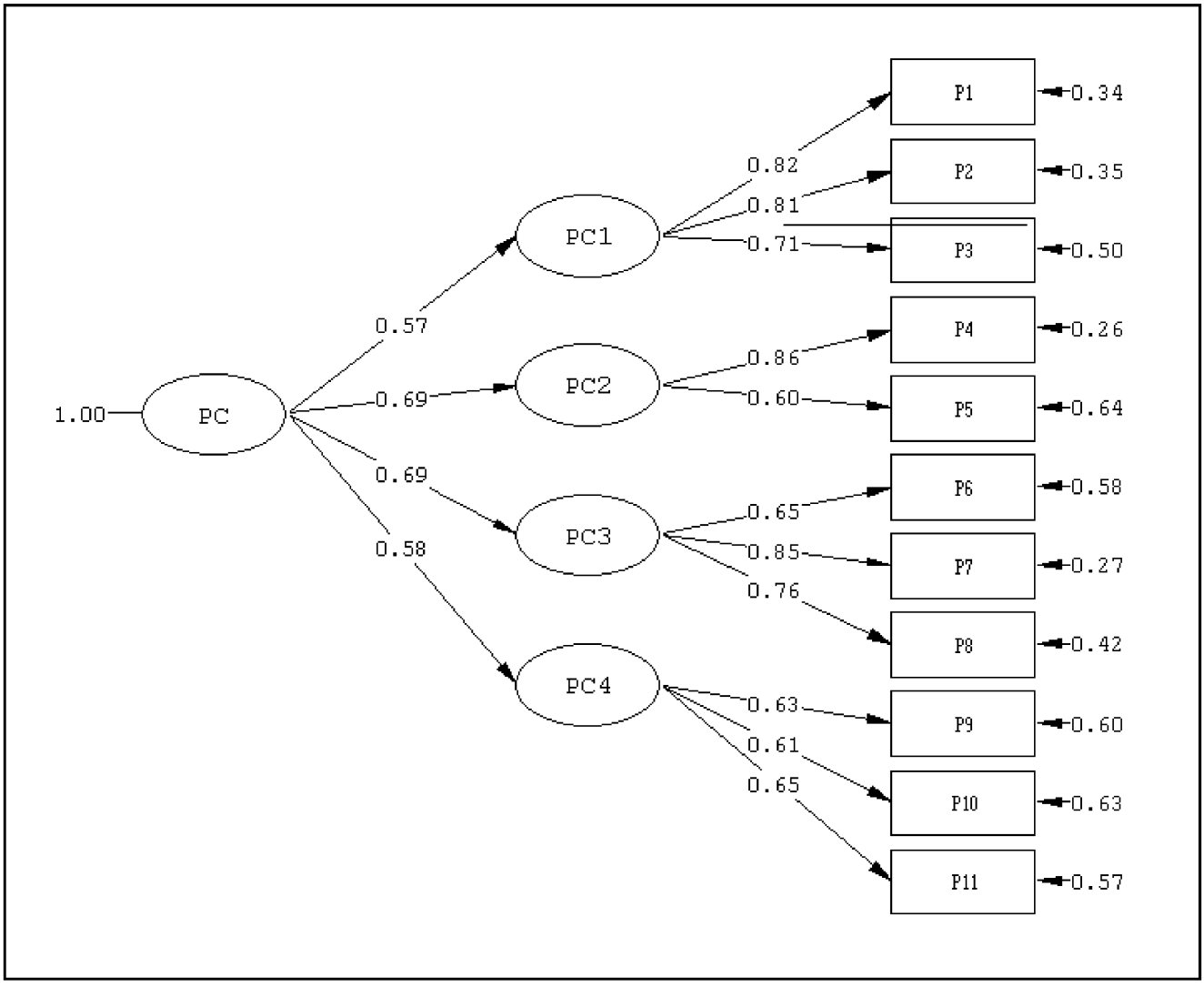

Figure 2. Second order CFA

model are consistent with the results from Stewart and Segars (2002) and Smith *et al.* (1996).

Figure 3 displays the measurement model for consumer trust. The overall model fit is significant. All items display appropriate loadings. The results are consistent with the findings of Gefen and Straub (2003).

Perceive privacy empowerment is a new construct. Figure 4 shows the first order measurement model for the consumer perceived privacy empowerment scale. The model fit indices are within acceptable parameters and the overall model fit is significant.

Path analysis and hypotheses testing

Next, the path model (which includes hypotheses) was examined. The fit indexes are within accepted thresholds: Chi-sq 2=3.88, CFI=0.99, RMR=0.035, RMSEA=0.068, GFI=0.99, AGFI=0.96, and NFI=0.98. Figure 5 shows the standardized LISREL path coefficients and the overall fit indexes. All the paths are significant at the 0.01 level. Table 4 contains the LISREL-calculated correlations among the constructs.

All five of our hypotheses were supported by the results of the path analysis.

Hypothesis 1: Increased privacy concerns negatively affect trust – Beta weight (path coefficient) −0.26, T=−4.06, p<0.001
Hypothesis 2: Perceived privacy empowerment negatively affects privacy concern – Beta weight −0.56, T=−9.88, p<0.001
Hypothesis 3: Perceived privacy empowerment positively affects trust – Beta weight 0.38, T=5.84, p<0.001
Hypothesis 4: Familiarity positively affects trust – Beta weight 0.15, T=2.75, p<0.01
Hypothesis 5: Familiarity positively affects empowerment – Beta weight 0.30, T=4.66, p<0.001

One interesting point to notice in this study is the scale of coefficients in the results. The standardized coefficient

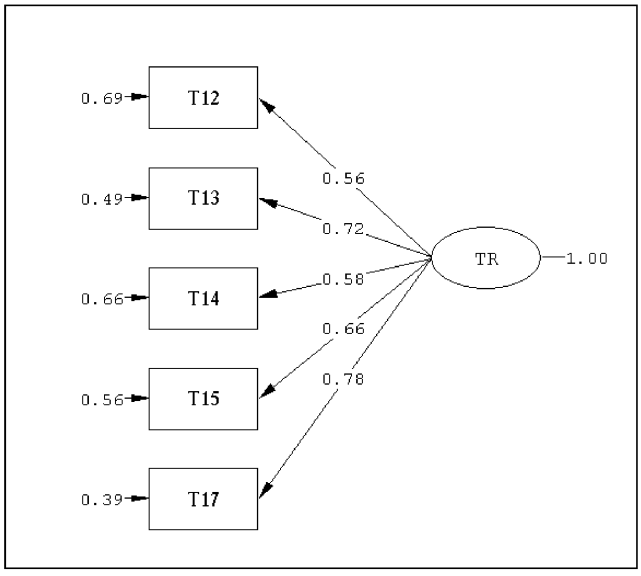

Figure 3. The measurement model for consumer trust
Notes: Normal Theory Weighted Least Squares Chi-Square=8.29 (p=0.14), Root Mean Square Error of Approximation (RMSEA)= 0.055, Normed Fit Index (NFI)=0.98, Comparative Fit Index (CFI)= 0.99, Goodness of Fit Index (GFI)=0.99, Adjusted Goodness of Fit Index (AGFI)=0.96

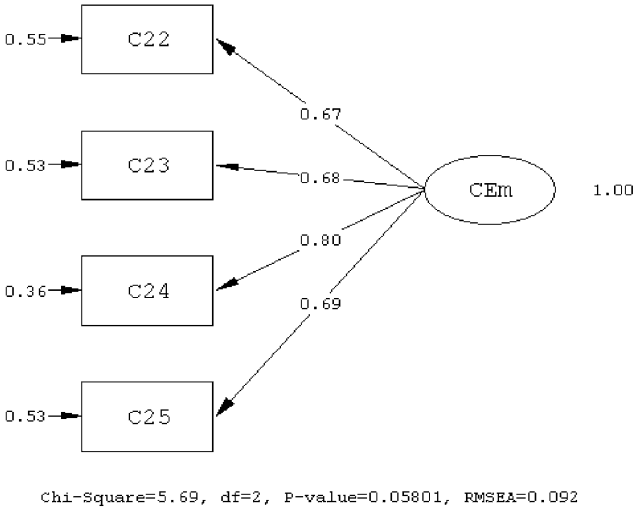

Figure 4. First order measurement model for the consumer perceived privacy empowerment scale
Notes: Root Mean Square Error of Approximation (RMSEA) = 0.092, Normal Theory Weighted Least Squares Chi-Square = 5.69 (p = 0.058), Goodness of Fit Index (GFI) = 0.99, Adjusted Goodness of Fit Index (AGFI) = 0.94, Normed Fit Index (NFI) = 0.98, Comparative Fit Index (CFI) = 0.99

for the direct effect between perceived privacy empowerment and trust is 0.38, which is more than double for the value of standardized coefficient, i.e. 0.15, between familiarity and trust. The total effects of the two constructs follow a similar pattern. The total effect of empowerment on trust is equal to the direct effect plus

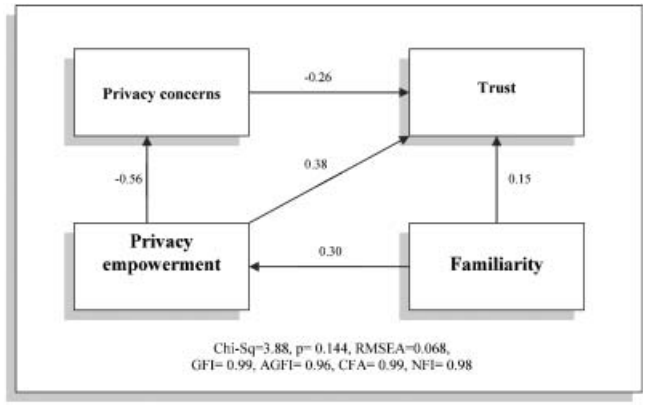

Figure 5. Standardized LISREL solution

Table 4. Standardized correlation matrix

	Privacy concerns	*Trust*	*Familiarity*	*Consumer empowerment*
Privacy concerns	1.000			
Trust	−0.482	1.000		
Familiarity	−0.062	0.285	1.000	
Consumer empowerment	−0.556	0.574	0.301	1.000

the sum of all indirect effects i.e., 0.38+(−0.56*−0.26)=0.53. Familiarity also has a significant indirect effect on trust via perceived consumer empowerment. The total effect of familiarity is 0.15+(0.30*0.38)+(0.30*0.56*0.26)=0.31. Familiarity has been considered an important precursor to trust. But our study shows that empowerment has a larger impact than familiarity on building consumer's trust. We should not downplay the importance of familiarity however. A certain amount of familiarity is necessary in order to be aware of empowering privacy policies on the part of the firm as indicated in the path analysis by the fact that familiarity has a significant positive affect on perceived empowerment. Both familiarity and perceived privacy empowerment are important constructs relating to trust in an e-commerce environment.

DISCUSSION

Trust and privacy

Previous research has demonstrated the importance of trust to e-commerce success (Gefen 2000, Hoffman *et al.* 1999, Howells 2005). Other studies have shown that privacy concerns can be a major cause of the lack of trust between the consumer and the firm (Culnan and Armstrong 1999). Our study introduced a new

construct, consumer privacy empowerment, and examined its impact on both privacy concern and trust. The results yield the following implications.

First the results indicate that privacy concerns have a significant negative effect on trust ($t=-4.06$, $p<0.001$). These results are consistent with the findings of Culnan and Armstrong (1999). Privacy issues have been rated as one of the most important barriers to the continued growth of e-commerce. The findings are also consistent with Liu *et al.* (2004) who found that privacy concerns decrease trust. Their study further found that the level of trust influenced several behavioural intentions including intention to purchase, intention to visit the site again and intention to recommend the site to others. The lack of consumer's trust in e-commerce is engendered primarily by the industry's documented failure to respond satisfactorily to mounting consumer concerns over information privacy in the electronic, networked world (Hoffman *et al.* 1999).

Our findings suggest that consumers lose trust in e-vendors when they perceive a threat to their privacy. They feel vulnerable, i.e., their private information is being used for unintended purposes, or by unauthorized persons, or may contain errors that might harm them in some way. Another factor may be Westin's (1967) concept of loss-of-control. Consumers may perceive that they do not have any control over their own personal information and it could be this lack of control, rather than any specific belief in the bad intentions of the vendor that may make them feel vulnerable.

Familiarity

Familiarity has been well studied in the e-commerce context. It has been shown to be positively linked with consumer's trust in e-vendors as well as consumer's willingness to transact (Gefen 2000). Our results are consistent with these previous findings. They indicate that familiarity can positively affect trust although the effect is not strong. Gefen and Straub (2003) also found that familiarity had a small but significant effect on trust. One reason that the effect of familiarity may not be stronger is that familiarity could conceivably impact trust in either direction. It is probably not familiarity per-se that positively affects trust but rather familiarity or previous experience with trustworthy firms that has that effect whereas familiarity with unscrupulous firms or negative previous experience is likely to have a negative effect on trust.

Perceived privacy empowerment

Consumer privacy empowerment was the focus of this research. We have noted above the importance of trust in e-commerce and the negative effect that privacy concerns have on trust. Westin (1967) contends that lack of control is at the heart of concerns over privacy. If that is true then the perception of being in control of your personally identifiable information would seem the logical antidote to the privacy concerns that impair trust. The results of this study support that contention.

Empowerment is positively related to trust in two ways. Perceived privacy empowerment has a significant negative effect on privacy concern ($t=-9.88$, $p<0.001$). In other words, an increase in the perception of privacy empowerment (e.g., control) leads to a decrease in the level of privacy concern. Thus empowerment positively affects trust, through an indirect effect, by lowering privacy concern. This result is consistent with the findings of Olivero and Lunt (2004) who found that increased levels of concern over privacy resulted in a decrease in trust and an increase in the demand for control. Our findings suggest that those firms which meet the demand for control through empowering the consumer are rewarded with lower levels of privacy concern and increased trust.

Empowerment also has a direct positive effect on trust ($t=5.84$, $p<0.001$). Lee *et al.* (2005) studied signalling in e-commerce. Although not investigating privacy empowerment directly, their results did indicate that the publication of a privacy policy on a website did act as a signal to the consumer that resulted in an increase in the probability of purchase. A privacy policy promising to keep customer's personal information private may be regarded as a signal of integrity because it conforms to customer's views of acceptable behaviour regarding their personal information (Lee *et al.* 2005). Our findings suggest that policies that provide consumers with privacy empowerment may operate in the same way.

Implications for practitioners

These results have an important implication for practitioners. Earlier studies have shown that companies can gain competitive advantage by behaving ethically, i.e. by letting users know what information they will collect, how they will collect, and for what purposes they will use that information (Culnan and Armstrong 1999). Trustworthiness has also been shown to be a source of competitive advantage (Barney and Hansen 1994). Our findings suggest that by behaving ethically, and empowering consumers to control their private information, a firm may be able to create a competitive advantage by increasing customer trust.

We suggest that two actions are required in order for a firm to take advantage of the implications of this research. First a firm can increase actual consumer privacy empowerment by adopting policies that delegate control over decisions related to private information to the consumer. Second the firm should communicate

these empowering policies in a way that builds a sense of empowerment in the mind of the consumer and thereby increases perceived privacy empowerment. For example, the *access* portion of the privacy statement should tout the consumer's right to see and correct personal information in addition to providing explicit guidelines on how to access and correct erroneous information.

It is our opinion that the traditional language used in privacy statements may not be the best way to communicate these policies and their implications. An argument can be made that the traditional language used in privacy policies does not engender trust, so much as require it. For those firms whose privacy statements do not provide the consumer with *choice* and *access*, the other portions of the privacy statement may actually increase privacy concern. The *notice* portion may list several possible ways that private information could be abused (i.e. unrelated marketing, sold to third parties etc). This may serve only to sensitize the consumer to potential risks they had not previously considered. Furthermore, a firm's promise not to engage in a specific behaviour seems to us to require trust on the part of the consumer rather than to engender it. New wording or methods should be adopted to create a sense of control on the part of the consumer over their private information. By delegating control to the consumer, the firm will signal its trustworthiness and at the same time reduce the amount of trust that the consumer is required to place in the ethical intentions of the firm. Such policies should limit the feeling of vulnerability on the part of the consumer and make it easier to trust the firm.

Limitations

It is important to note that the sample for this study included only people who had made at least one Internet purchase. In addition, all of the participants had visited the website that they used for the basis of their response. McKnight *et al* (2004) noted that the factors that affect trust shift depending on the stage of the relationship between the consumer and online vendor. For example before visiting a site, disposition to trust and reputation advertising are more important trust factors. After visiting the website page quality becomes more important. McKnight *et al.* (2004) divide the initial trust building period into two stages: an *introductory* stage and an *exploratory* stage. During the introductory stage, users have not yet experienced a specific website and are trying to assess the site based on second-hand information. This stage ends when the user first visits the site. Those who visit the site enter the exploratory stage in which the user interacts with the website and makes a new assessment based on first-hand experience. In this study all respondents had undergone the *exploratory* stage. Therefore, the findings relating to the effects of various factors on trust should only be generalized to consumers at this stage of the purchasing relationship. The relationships between factors affecting trust might be different for consumers who had never purchased from the Internet or those who have not yet visited the site in question.

CONCLUSIONS

In this study we introduced a new construct, perceived consumer privacy empowerment, and developed hypotheses predicting the relationships between empowerment, familiarity, privacy concern and trust in an e-commerce context. In order to test these hypotheses we developed and validated an instrument to measure perceived privacy empowerment. Utilizing the new instrument along with previously developed scales, we performed a survey and statistical analysis. The results of the study expanded the nomological net associated with trust. The most salient new findings of this study demonstrate that increasing perceived privacy empowerment leads to a reduction in privacy concern and increase in trust.

These finding also have important implications for practitioners many of whom are searching for ways to minimize consumer's privacy concern and increase consumer trust in their websites. The results of this study suggest that a useful strategy for an e-vendor interested in increasing consumer trust is to build a sense of privacy empowerment in the mind of the consumer.

References

Agarwal, R. and Karahanna, E. (2000) 'Time Flies when You're Having Fun: Cognitive Absorption and Beliefs about Information Technology Usage', *MIS Quarterly* 24: 665–94.

Anderson, J. C. and Gerbing, D. W. (1988) 'Structural Equation Signalling in Practice: A Review and Recommended Two-Step Approach', *Psychology Bulletin* 103(3): 411–23.

Barney, J. B. and Hansen, M. H. (1994) 'Trustworthiness as a Source of Competitive Advantage', *Strategic Management Journal* 15: 175–90.

Bessen, J. (1993) 'Riding the Marketing Information Wave', *Harvard Business Review* 71(5): 150–60.

Blau, P. M. (1964) *Exchange and Power in Social Life*, New York: Wiley.

Bloom, P. N., Milne, G. R. and Alder, R. (1994) 'Avoiding Misuses of Information Technologies: Legal and Societal Considerations', *Journal of Marketing* 58(1): 98–110.

Chin, W. W. (1998) 'Issues and Opinion on Structural Equation Signalling', *MIS Quarterly* 22(1): vii–xvi.

Chow, S. and Holden, R. (1997) 'Toward an Understanding of Loyalty: The Moderating Role of Trust', *Journal of Managerial Issues* 9(3): 275–98.

Clarke, R. (1999) 'Internet Privacy Concerns Confirm the Case for Intervention', *Communications of the ACM* 42: 60–7.

Compeau, D. R., Higgins, C. A. and Huff, S. (1999) 'Social Cognitive Theory and Individual Reactions to Computing Technology: A Longitudinal Study', *MIS Quarterly* 23(2): 145–58.

Culnan, M. J. and Armstrong, P. K. (1999) 'Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation', *Organizational Science* 10(1): 104–15.

Federal Trade Commission (2000) 'Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress', Washington DC, online at: http://www.ftc.gov/reports/privacy2000/privacy2000.pdf [accessed 21 April 2006].

Ford, P. (2000) 'Is the Internet Changing the Relationship Between Consumers and Practitioners?', *Journal of Health Care Quality* 22(5): 1–3.

Fried, C. (1984) 'Privacy', in F. D. Shoeman (ed.) *Philosophical Dimensions of Privacy*, New York: Cambridge University Press.

Fukuyama, F. (1995) *Trust: Social Virtues and the Creation of Prosperity*, New York: The Free Press.

Galanxhi, H. and Nah, F.-H. (2006) 'Privacy Issues in an Era of Ubiquitous Commerce', *Electronic Markets – The International Journal* 16(3): 222–32.

Gefen, D. (2000) 'E-Commerce: The Role of Familiarity and Trust', *Omega* 28(6): 725–37.

Gefen, D. (2002) 'Customer Loyalty in E-Commerce', *Journal of the Association of Information Systems* 3: 27–51.

Gefen, D. and Straub, D. W. (2003) 'Trust and TAM in Online Shopping: An Integrated Model', *MIS Quarterly* 27(1): 51–90.

Gellman, R. (2002) 'Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete', (March 26), online at: http://www.epic.org/reports/dmfprivacy.html [accessed 21 April 2006].

Grewal, D., Munger, J. L., Iyer, G. and Levy, M. (2003) 'The Influence of Internet-Retailing Factors on Price Expectations', *Psychology & Marketing* 20(6): 447–93.

Hair, J. F. Jr., Anderson, R. E. and Black, W. C. (1998) *Multivariate Data Analysis*, 5th edn, New Jersey: Prentice Hall.

Hart, C. W. and Johnson, M. D. (1999) 'Growing the Trust Relationship', *Marketing Management* 8(1): 8–19.

Hoffman, D. L., Novak, T. P. and Peralta, M. (1999) 'Building Consumer Trust Online', *Communications of the ACM* 42(4): 80–5.

Hong-Youl, H. and Perks, H. (2005) 'Effects of Consumer Perceptions of Brand Experience on the Web: Brand Familiarity, Satisfaction and Brand Trust', *Journal of Consumer Behavior* 4(6): 438–52.

Howells, G. (2005) 'The Potential and Limits of Consumer Empowerment by Information', *Journal of Law and Society* 32(3): 349–70.

Jarvenpaa, S., Tractinsky, N. and Vitale, M. (2000) 'Consumer Trust in an Internet Store', *Information Technology and Management* 1: 45–71.

Kirmani, A. and Rao, A. R. (2000) 'No Pain, No Gain: A Critical Review of the Literature Signalling Unobservable Product Quality', *Journal of Marketing* 64(2): 66–79.

Langer, E. J. (1983) *The Psychology of Control*, Beverly Hills: Sage.

Lee, B., Ang, L. and Dubelaar, C. (2005) 'Lemons on the Web: A Signaling Approach to the Problem of Trust in Internet Commerce', *Journal of Economic Psychology* 26: 607–23.

Lee, M. K. O. and Turban, E. (2001) 'A Trust Model for Consumer Internet Shopping', *International Journal of Electronic Commerce* 6(1): 75–91.

Liao, Z. and Cheung, M. T. (2001) 'Internet-Based E-Shopping and Consumer Attitudes: An Empirical Study', *Information and Management* 38: 299–306.

Liu, C., Marchewka, J. T., Lu, J. and Yu, C. (2004) 'Beyond Concern: A Privacy-Trust-Behavioral Intention Model of Electronic Commerce', *Information & Management* 42: 127–42.

McKnight, D. H. and Chervany, N. L. (2002) 'What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology', *International Journal of Electronic Commerce* 6(2): 35–59.

McKnight, D. H., Kacmar, C. J. and Choudhury, V. (2004) 'Shifting Factors and the Ineffectiveness of Third Party Assurance Seals: A Two-Stage Model of Initial Trust in a Web Business', *Electronic Markets – The International Journal* 14(3): 252–66.

Olivero, N. and Lunt, P. (2004) 'Privacy Versus Willingness to Disclose in e-Commerce Exchanges: The Effect of Risk Awareness on the Relative Role of Trust and Control', *Journal of Economic Psychology* 25: 243–62.

Petersen, A. (2001) 'Private Matters: It Seems That Trust Equals Revenue, Even Online', *Wall Street Journal*, 12 February, R24, R31.

Price, L. and Dawar, N. (2002) 'The Joint Effects of Brands and Warranties in Signalling New Product Quality', *Journal of Economic Psychology* 23: 165–90.

Quelch, J. A. and Klien, L. R. (1996) 'The Internet and International Marketing', *Sloan Management Review*, Spring, 60–75.

Ranganathan, C. and Grandon, E. (2002) 'An Exploratory Examination of Factors Affecting Online Sales', *Journal of Computer Information Systems*, Spring, 87–93.

Roboff, G. and Charles, C. (1998) 'Privacy of Financial Information in Cyberspace: Banks Addressing What Consumers Want', *Journal of Retail Banking Services* 20(3): 51–6.

Schoder, D. and Haenlein, M. (2004) 'The Relative Importance of Different Trust Constructs for Sellers in the Online World', *Electronic Markets – The International Journal* 14(1): 48–57.

Sheehan, K. B. and Hoy, M. G. (1998) 'Privacy and On-Line Consumers: Comparisons with Traditional Consumers and

Implications for Advertising Practice', *Proceedings of the 1998 American Academy of Advertising Conference*, Pullman WA, Washington State University, 77–8.

Sheth, J. N. and Pravatiyar, A. (2000) 'Relationship Marketing in Customer Markets: Antecedents and Consequences', in *Handbook of Relationship Marketing*, Thousand Oaks, Sage.

Smith, J. H., Milberg, S. and Burke, S. J. (1996) 'Information Privacy: Measuring Individuals Concerns About Organizational Practices', *MIS Quarterly* 20(6): 167–96.

So, M. and Sculli, D. (2002) 'The Role of Trust, Quality, Value and Risk in Conducting e-business', *Industrial Management and Data Systems* 102(9): 503–12.

Spreitzer, G. M. (1995) 'Psychological Empowerment in the Workplace: Dimensions, Measurement, and Validation', *Academy of Management Journal* 38(5): 1442–65.

Stewart, K. A. and Segars, A. H. (2002) 'An Empirical Examination of the Concern for Information Privacy Instrument', *Information Systems Research* 13(1): 36–49.

Tan, Y. and Thoen, W. (2001) 'Toward a Generic Model of Trust for Electronic Commerce', *International Journal of Electronic Commerce* 5(2): 61–74.

Tavani, H. T. and Moor, J. H. (2001) 'Privacy Protection, Control of Information and Privacy Enhancing Technologies', *Computers and Society*, March, 6–11.

Tedeschi, R. (2000) 'E-Commerce Report: Some Online Sellers are Hiring Prominent Auditors to Verify their Privacy Policies and Increase Trust', *The New York Times*, 18 September, C12.

Thomas, K. W. and Velthouse, B. A. (1990) 'Cognitive Elements of Empowerment', *Academy of Management Review* 15: 666–81.

Wathieu, L., Brenner, L., Carmon, Z., Drolet, A., Gourville, J., Muthukrishnan, A. V., Novemsky, N. and Wu, G. (2002) 'Consumer Control and Empowerment: A Primer', *Marketing Letters* 13(3): 297–305.

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