Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model

Chechen Liao,1, Chuang-Chun Liu,2, Kuanchin Chen

1 Department of Information Management, National Chung Cheng University, Ming-Hsiung, Chia-Yi 62102, Taiwan
2 Department of Business Information Systems, Western Michigan University, 3344 Schneider Hall, Kalamazoo, MI 49008-5412, United States

ARTICLE INFO

Article history:
Received 24 February 2010
Received in revised form 2 July 2011
Accepted 2 July 2011
Available online 8 July 2011

Keywords:
E-commerce
Privacy concerns
Privileged information search
Risk
Internet literacy
Social awareness
Disposition to trust

ABSTRACT

Much interest in privacy and trust studies is about shopping, but privacy research in other forms of online activities is beginning to emerge. This study examined the antecedents of privacy, trust and risk as well as their joint effect on two similar but fundamentally different activities: online transactions and retrieval of privileged information. Both activities involve the delivery of private user information, but the latter gives some leeway for users to control (or even falsify) their true identity. User shopping experience in the present study moderated the relationships and strengths of constructs. The effect of Internet literacy, social awareness and disposition to trust on privacy concern and trust was weaker for experienced shoppers. Privacy concern, trust and risk assessment played a lesser role on the two activity variables for those who were more experienced. Perceived privacy risk stood out as a strong antecedent for respondents in both experience groups, but the effect of Internet literacy, social awareness and disposition on trust was statistically insignificant for the same group. Further practical and managerial implications are provided.

© 2011 Elsevier B.V. All rights reserved.

1. Introduction

Sixty-two percent of Internet users are concerned about their online privacy (Han and Maclaurin 2002). Studies (Gefen et al. 2003a, Hoffman et al. 1999, Pavlou and Gefen 2004) have shown that trust and privacy concerns continue to be two main components for the decision to disclose personal information on the Internet. Both trust (Chau et al. 2007, Corbitt et al. 2003, Eastlick et al. 2006, Slyke et al. 2006) and privacy concerns (Dyke et al. 2007, Eastlick et al. 2006, Kim 2008, Liu et al. 2005, Malhotra et al., 2004) are also frequently cited in the literature as the main reasons for an individual's lack of interest to establish an online relationship with merchants.

Privacy and trust have received much attention in the literature for their relationships with online transactions, but today's privacy and trust issues are not limited to only activities relating to online transactions. Many activities on the Internet (games, information sharing, insurance quotes, surfing, etc.) also have an effect on one's privacy. In this study, we focus on the consumer's intention to engage in two types of activities (online transactions and online privileged information searching) that require some form of personal identifiable information.

Intention to transact refers to the willingness to be engaged in monetary transactions, which many times involve the exchange of accurate personal or private information. Today, many online non-monetary activities also involve the exchange of personal or private information. For example, using web sites that provide personalized stock quotes, insurance rates, loan comparisons, availability of services and credit reports all require certain personal or private information, but such activities do not necessarily require a direct monetary exchange with the web site. Some may lead to future purchases, but some may just be for personal reasons. These activities provide privileged information to the recipients, that involves the kind of information or advantage available to certain groups of people who willfully opt for the services by entering into a membership, subscription, affiliation or any sort of non-obligated service engagement. These activities are frequently associated with comparison shopping, pre-purchase information gathering and post-purchase service quotes. Thus, we propose the intention to retrieve privileged information as a variable that refers to an individual's willingness to provide personal or private information in exchange for certain privileged or customized information from the Internet. Similar to willingness to transact online, this variable involves the exchange of personal and private information, thus several constructs (e.g., privacy, trust, and perceived risk) relating to intention to transact may also
apply. This is because the risk involved in such exchange of private information is not just limited to a possible economic loss (as Dinev and Hart 2006a, and others have pointed out), but it may also be in the form of loss of private information or even identity. As Culnan and Armstrong (1999) noted, individuals surrender a certain degree of privacy when they disclose personal information. Privacy concerns are heightened and trust is lowered when consumers find it difficult to control their own private information from misuse or unauthorized distribution once it leaves their own computers. This perception of uncertainty causes hesitation for a consumer to disclose his or her personal information. Numerous e-commerce studies have focused on monetary transactions (Gefen et al. 2003a, Gupta and Kim 2007, Lee and Turban 2001). Yet, very few studies have examined the impact of behavior and privacy uncertainty (privacy concerns, privacy risk and trust) for activities other than monetary transactions. Surprisingly, even fewer studies have focused on the role of privacy and trust on information searching, especially the type of information that require personal information. Since privileged information searching does not always include the delivery of goods to an individual's physical residence or require precise contact information, accuracy of user information is not always strictly required or even validated. This offers consumers opportunities to control or fake their personal information before it is sent to the web site (Chen and Rea 2004). Little is known for the inter-twined effect of trust, privacy concerns and perceived risk on intentions to transact and retrieve privileged information online when both these latter activities are considered together. As such, a model that integrates variables relating to these two activities warrants further examination.

This study is designed to build an integrated model derived from existing theories to examine the two forms of activities (transactions and retrieval of privileged information). This serves two objectives. First, the study aims to distinguish two popular online activities that bear different requirements of private information. The result is expected to shed light on the effects of antecedent variables on the two activities when both activities are taken into consideration. Second, a series of verification including model comparison with and without moderation measures lends itself both theoretical and practical contributions. Among the salient factors studied in this research are Internet literacy, social awareness and perceived risk, privacy concerns, and trust.

2. Literature

2.1. Privacy concerns

Westin (1967) defined information privacy as the ability to control how an individual's personal information is acquired and used. Several researchers have tailored the definition toward the informational aspect of privacy rather than its physical, spatial, and behavioral aspects, and refer to privacy as an individual's ability to personally control information about oneself (Awad and Krishnan 2006, Dinev and Hart 2006b). There is a growing concern about how much individuals are able to protect their personal information. As a result, privacy has continued to attract attention in the literature, especially in e-commerce related research. Dinev et al. (2006) define privacy concerns as concerns about possible loss of privacy as a result of a voluntary or surreptitious information disclosure to a web site. Privacy concerns result from three processes: (1) interaction with information technology (IT), which requires some level of technology literacy, (2) a social process of communication and transaction with sometimes anonymous or little known social entities in the Internet environment (Dinev and Hart 2006b), and (3) an uncertainty reduction mechanism in the realm of e-commerce.

Privacy issues include unauthorized sharing of personal information, spam from the online retailer, and disclosure of the patterns of online customer shopping behavior (Miyazaki and Fernandez 2001). In online shopping, while sellers take advantage of personal information to gain an edge, buyers often view this as an invasion of privacy (Culnan and Armstrong 1999). Table 1 summarizes two popular types of measures for privacy concerns: general versus specific. General privacy concerns refer to the privacy concerns in general, while specific privacy concerns apply to specific situations or entities (Li et al. 2010).

Malhotra et al. (2004) found that the second-order Internet users’ information privacy concerns (IUPI) factor, which consists of three first-order dimensions (collection, control, and awareness), exhibited desirable psychometric properties in the context of online privacy. In addition, Chen and Rea (2004) tested Internet users’ ability to control their private information and the relationship of privacy controls with two types of privacy concerns: unauthorized secondary use and concerns about giving out private information. Furthermore, Slyke et al. (2006), Dyke et al. (2007), Korzan and Boswell (2008) and Xu and Gupta (2009) examined the role of consumers’ concerns for information privacy (CFIP) on their behavioral intention to engage in online transactions. In summary, privacy is a major concern when online customers make a transaction (Udo 2001).

2.2. Trust

Mayer et al. (1995) defined trust as, “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the truster, irrespective of the ability to monitor or control that other party”. Trust is crucial in many transactional relationships, especially those containing an element of risk, such as online transactions (Reichheld and Schefter 2000).

In the relationship marketing, trust is generally viewed as an essential ingredient for a successful relationship (Moorman et al. 1993, Morgan and Hunt 1994). Trust is seen as a form of confidence on a partner as a whole (Moorman et al. 1993) and the partner's reliability and integrity (Morgan and Hunt 1994). Previous studies have also shown that trust is the most critical factor in explaining the success of e-commerce (Jarvenpaa et al. 2000, Kim et al. 2010, McKnight et al. 2002).

In the context of consumer trust in e-commerce, McKnight et al. (2002) defined trust as “one believes in, and is willing to depend on, another party.” Trust is driven by past experience, long-term orientation, positive trusting stance, and feeling of control (Jarvenpaa and Tractinsky 1999). Jarvenpaa et al. (1998) found that trust consists of three distinct factors: ability, integrity and benevolence. These three beliefs affect the members of virtual team’s trusting behavioral intentions, meaning their willingness to depend on other team members. Jarvenpaa et al. (2000) noted that trust is an important factor in any relationship in which the truster does not have direct control over the actions of a trustee (e.g., e-vendor). In addition, Gefen (2002) defined trust as a single dimensional construct dealing with a consumer’s assessment that the e-vendor is trustworthy. Gefen et al. (2003a) pointed out that trust consists of four distinct dimensions: integrity, benevolence, ability, and predictability. In recent years, most of studies measured trust by all or parts of these four dimensions (Chow and Angie 2006, Kim and Ahn 2006, Slyke et al. 2006). A summary of findings is in Table 2.

2.3. Intention to retrieve privileged information

A popular focus of privacy and trust studies is how the two concepts relate to online transactions (Gefen et al. 2003a, Pavlou and
have raised several concerns for user privacy (Hoadley et al. 2010). A and the subsequent levels and depth of online disclosures, has the popularity of online social networks, such as Facebook, MySpace. However, today's privacy and trust issues are not constrained to only online transaction activities. The risk involved for privileged information searching is more likely information risk, sometimes also called identity risk or privacy risk, as opposed to financial risks that also existing in online transactions.

### Table 2

Previous conceptualizations of trust.

<table>
<thead>
<tr>
<th>Authors</th>
<th>Trust conceptualization</th>
<th>Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jarvenpa et al. (1998)</td>
<td>Willingness of a party to be vulnerable to the actions of another party</td>
<td>Ability, integrity and benevolence</td>
</tr>
<tr>
<td>Jarvenpa and Tractinsky (1998)</td>
<td>Ability, integrity and benevolence</td>
<td>Overall trust combined with integrity, and caring</td>
</tr>
<tr>
<td>Jarvenpa et al. (2000)</td>
<td>A governance mechanism in buyer–seller relationships</td>
<td>Overall trust combined with integrity, and caring</td>
</tr>
<tr>
<td>Gefen (2002)</td>
<td>Willingness to deped</td>
<td>Overall trust</td>
</tr>
<tr>
<td>McKnight et al. (2002)</td>
<td>Trusting beliefs dealing with benevolence, competence, honesty, and predictability</td>
<td>Conceptual</td>
</tr>
<tr>
<td>Corbitt et al. (2003)</td>
<td>Trusting beliefs dealing with competence, predictability, and goodwill</td>
<td>Dependable, reliable, honest and trustworthy</td>
</tr>
<tr>
<td>Gefen et al. (2003a)</td>
<td>Willingness to deped</td>
<td>Competence, predictability, and goodwill</td>
</tr>
<tr>
<td>Pavlou and Gefen (2004)</td>
<td>Appropriate conditions are in place to facilitate transaction success with the marketplace's sellers</td>
<td>Integrity, benevolence, ability, and predictability</td>
</tr>
<tr>
<td>Chow and Angie (2006)</td>
<td>Willingness of a party to be vulnerable to the actions of another party</td>
<td>Overall trust combined with integrity, ability, beneficence</td>
</tr>
<tr>
<td>Kim and Ahn (2006)</td>
<td>The expectation that an exchange partner will not engage in opportunistic behavior</td>
<td>Benevolence and integrity</td>
</tr>
<tr>
<td>Slyke et al. (2006)</td>
<td>As the trustee’s expectations about the ability, benevolence, and integrity of the merchant</td>
<td>Overall trust combined with integrity, ability, beneficence</td>
</tr>
<tr>
<td>Pavlou et al. (2007)</td>
<td>Willingness to deped</td>
<td>Overall trust</td>
</tr>
<tr>
<td>Sledgianowski and Kulviwat (2009)</td>
<td>Perceived trust in an institutional context</td>
<td>Honesty, responsibility, understanding, caring, and professionalism</td>
</tr>
</tbody>
</table>

### 2.4. Purchase versus information retrieval

Purchase and information retrieval on the Internet have been shown to be theoretically distinct concepts (Gefen and Straub 2000, Shim et al. 2001). An online consumer might be a buyer in online shopping or an information seeker in information retrieval (Huang et al. 2004). The two concepts differ in several ways. For example, activities in many online transactions involve the transfer of user's identity or even personal information sometimes without a user's knowledge. Even though a given transaction may not require personal information from a consumer directly, it pulls such information from other sources (or from the merchant's own database) for other promotional reasons. Accuracy of user information is typically required for a successful online transaction, but such a requirement of information accuracy is not necessarily a must to access privileged information online. Therefore, consumers are given much leeway to exercise several forms of privacy control (Chen and Rea 2004), including forging of the private information.
Even scarcer are the studies that look at these two variables and their antecedent variables together in an integrated model.

3. Theoretical foundations

Urban et al. (1999, p. 9) stated: “If customers do not trust that their personal data will be kept private and that payment is secured and executed only with appropriate authorization, they will not use the Internet.” Internet privacy concern and trust are inextricably linked and when combined, may actually have an effect on an individual’s intention to purchase online. A number of factors including personality based privacy attitudes, privacy uncertainty, and various trust-establishing factors have been identified that all play a role in the privacy calculus of Internet users (Kobsa 2007). The variables of behavioral and privacy uncertainty (e.g., privacy concerns, perceived risk and trust) are posited as key drivers for e-commerce acceptance (Gefen et al. 2003a, Pavlou and Gefen 2004, Pavlou et al. 2007, Slyke et al. 2006, Tan and Thoen 2001, Xu and Gupta 2009).

For example, trust and perceived risk both influence trust intentions (Pavlou and Gefen 2004). Similarly, trust, perceived risk and privacy concerns were found to have a direct effect on transaction intentions (Dinev and Hart 2006a). Gefen (2000) found that the relationship between disposition to trust and purchase intention was mediated by trust, thereby confirming the effects of trusting belief (disposition to trust) to trusting behavior and then to the final purchase intention. Trust and perceived risk as the direct antecedent variables for transaction intentions are also reported in Gefen and Pavlou (2006) when all levels of perceived regulatory effectiveness of online marketplaces are considered. Literature supports privacy concerns, trust and perceived risk as predictor variables for individuals’ purchase intentions online.

Although literature supports perceived risk as an antecedent variable for purchase intentions, its relationship with privacy concern and trust is quite mixed. This is especially true between perceived risk and trust. Empirical evidence is available for perceived risk to be the antecedent variable for trust (Dinev and Hart 2006a, Bansal et al. 2010, Corbitt et al. 2003, Thoen 2001, Cheung and Lee 2003), for trust to be the antecedent of perceived risk (Pavlou 2003, Gefen 2002, Gefen and Pavlou 2006), and a two-way relationship (see Lim (2003) for a review). Added to the complexity is that perceived risk is measured differently across studies. Featherman and Pavlou’s work (2003) suggests that the general concept of perceived risk actually consists of multiple facets, including performance risk, financial risk, time risk, psychological risk, social risk, privacy risk as well as overall risk. Examples of studies that measured these risk facets are: Pavlou and Gefen (2004), Pavlou (2003), Gefen (2002) and Gefen and Pavlou (2006) for the perceived overall risk of using a specific seller; Xu et al. (2008) and Dinev and Hart (2006a) for the perceived privacy risk in general; Malhotra et al. (2004) for the perceived privacy risk specific to a firm; Grabner-Kraeuter and Faulrant (2008) and Chang and Chen (2008) for a mixed type of financial, privacy and performance risks. In sum, two popular trends for perceived risk and its relationship with trust emerge depending on how perceived risk is measured. Studies that treat risk as privacy risk (or information risk) in general support perceived risk as an antecedent of trust, whereas studies of perceived risk for a specific firm or as a mixed type of risk support perceived risk as a predictor of trust. In this present study, we are interested in examining the first form of risk (privacy risk) and its relationship with others.

4. Research model and hypotheses

Fig. 1 shows the research model. This integrates variables from existing studies including (a) individual characteristics (Internet literacy, social awareness, and trusting disposition), and (b) behavioral and privacy uncertainty (privacy concerns, privacy risk and trust) with the objective of better explaining customer acceptance and adoption of two online activities (transactions and retrieval of privileged information).

4.1. Antecedents of privacy concerns

Challenges a typical online customer may encounter include establishing an Internet connection, orienting self-efficiently on a website, completing an online transaction, submitting personal information, dealing with deceptions and so on (Grazzioli and Jarvenpaa 2003). All these activities require substantial knowledge and skills in order to protect one’s privacy, and information one would rather not disclose, or permit to be further disclosed by an online retailer (Dinev and Hart 2006b).

Internet literacy is closely related to computer literacy. The standard dictionary defined of computer literacy as the ability to use a computer and its software to accomplish practical tasks. Following Dinev and Hart (2006b), Internet literacy can be characterized as the ability to use a network-connected computer and Internet applications to accomplish practical tasks. They found that Internet literacy had a negative effect on Internet privacy concerns. The more consumers are Internet literate, the less concerned they will be about privacy. This is due to their comfort level with protecting their computers and controlling intrusive technologies as they gain more experience and become more Internet literate.

Social, technical, and personal issues are among the many challenges for Internet users. Burn and Loch (2001) suggest that among the social issues, trust, privacy, security, governance, censorship, and restrictions have been identified as having a highest priority. In the literature, social awareness is defined as passive involvement and raised interest in social issues. Greene and Kaminura (2003) defined social awareness as naming the problem, speaking out, consciousness raising, and researching. Internet users who are more socially aware tend to know more about the privacy risks, privacy debate and privacy policies associated with the Internet, and the legal implications of privacy invasions and identity theft. They are better aware of the importance of privacy in social life. The stronger an individual is aware of the society, the more likely he or she will consider privacy as an important societal value. As a result, the individual will also presumably be more concerned about privacy (Dinev and Hart 2006b).

Studies have found that perceptions of risk concerning online retailers and their business practices are related to privacy
concerns. For example, Grant (2005) found several major causes for teens’ privacy concerns on the Internet, including such factors as unsolicited commercial messages, being tracked for their online activities, and loss of control of their privacy information. Support for perceived risk as the predictor of privacy concerns are also found in studies, such as Youn (2009) and Bandopadhyay (2009). Technology tools have enabled opportunistic behaviors to easily collect, associate and share personal information on the Internet, which ultimately leads to a greater privacy risk. With heightened privacy risk due to factors outside of control of individuals, consumers are concerned about who has access to their personal information (Dinev and Hart 2006a, 2006b; Xu et al. 2008).

Therefore, the following hypotheses are proposed:

Hypothesis 1. Internet literacy will have a negative effect on privacy concerns.

Hypothesis 2. Social awareness will have a positive effect on privacy concerns.

Hypothesis 3. Perceived risk will have a positive effect on privacy concerns.

4.2. Antecedents of trust

Trust perception is interwoven with risk (McAllister 1995, Jarvenpaa et al. 2000, Tan and Thoen 2001). The relationship between perceived risk and trust has attracted much interest in the literature, but the empirical results for the type of relationship are still mixed. Lim (2003) provides a nice summary of the possible relationships including (a) perceived risk as a moderator between trust and intention to buy, (b) perceived risk and trust jointly affect the trusting behavior, (c) trust as the antecedent variable for perceived risk, and (d) perceived risk and trust have a two-way relationship between each other. Although the very last type of relationship shows a possibility for perceived risk to be an antecedent of trust, it is not until recently for the empirical evidence to appear in the literature.

Mayer et al. (1995) pointed out that the precise relationship between risk and trust is not very clear. They have made the following observations showing the complexity of the relationship between these two variables: “There is no risk taken in the willingness to be vulnerable (i.e., to trust), but risk is inherent in the behavioral manifestation of the willingness to be vulnerable. One does not need to risk anything in order to trust; however, one must take a risk in order to engage in trusting action. The fundamental difference between trust and trusting behaviors is between a willingness to assume risk and actually assuming risk. Trust is the willingness to assume risk; behavioral trust is the assuming of risk” (Mayer et al. 1995, p. 724). In recent years, several studies have suggested that a trusting belief is based on some degree of risk (Dinev and Hart 2006a, Bansal et al. 2010). Providing personal information to transact and retrieve privileged information on the Internet both involves certain degree of privacy risk and uncertainty. Based on Mayer et al.’s observations, one must take a privacy risk before a trusting action (to trust the merchant in order to transact and retrieve privileged information). Corbitt et al. (2003) initially hypothesized perceived risk as the antecedent of trust, but the correlation between the two variables was too low to warrant a relationship of any kind. However, other empirical evidence (e.g., Dinev and Hart 2006a, Tan and Thoen 2001, Tiangsoongnern 2007) is also available to support perceived privacy risk as the antecedent variable of perceived trust. Dinev and Hart (2006a, p. 64) pointed out especially that existing studies on perceived risk “... have not accounted for possible loss of personal information in their assessment of perceived risk; risk was either measured in general terms or emphasized the possibility of economic loss rather than privacy loss.” Therefore, we adopt this line of research in conceptualizing perceived risk as perception of risk resulting from a possible privacy loss (or loss of private information), as well as its relationship with trust, as follows:

Hypothesis 4. Perceived risk will have a negative effect on trust.

Disposition to trust is the general willingness to trust other people and a measure of an individual’s tendency to trust or distrust. McKnight et al. (2002) suggest that a person may have dispositional trust because they either believe in the general good nature of people, or they believe that they will achieve better outcomes by tending to trust people. Disposition to trust would influence trust in a specific other (specific organization or person), but only when novel situations arise in which the other and the situation are unfamiliar (Johnson-George and Swap 1982, McKnight et al. 1998). The online shopping environment is full of possibilities for a vendor to try out new promotional or service tools that are not commonly available with brick-and-mortar stores. For example, one-click shopping offered through Amazon.com and virtual account from Citibank are services available online that aim to improve shopping convenience and security. Some level of novelty is associated with these services. Evidence is also available to support disposition to trust as an antecedent variable of trust in e-commerce (Gefen 2000, McKnight and Chervany 2002). Therefore, in the Internet environment, we believe individuals with higher tendency to trust in general are more likely to trust electronic commerce. Hence, the following hypothesis is proposed:

Hypothesis 5. Disposition to trust will have a positive effect on trust.

4.3. Antecedents of intention to transact and retrieve privileged information

Risk has been found to affect the intention to conduct e-commerce transactions (Dinev et al. 2006, Featherman and Pavlou 2003, Jarvenpaa and Tractinsky 1999, Jarvenpaa et al. 2000, McKnight et al. 2002, Nicolaou and McKnight 2006, Pavlou 2003, Slyke et al. 2006). Because of this risk, individuals become hesitant to disclose personal information necessary to conduct online transactions. Privacy concerns, in turn, should be related to intention to provide personal information to transact on the Internet. Prior studies have argued that privacy concern is a key barrier to consumer e-commerce (Hoffman et al. 1999). The effect of privacy concerns on purchase-related behaviors from the direct marketing literature shows that concerns for privacy influence both information disclosure and purchase intentions (Phelps et al. 2001). Labuschagne and Elloff (2000) also suggested privacy concerns are likely to lower purchase intentions.

Hoffman et al. (1999) argued that lack of trust prevents consumers from engaging in online transactions because they may not transact with an online retailer that fails to convey a sense of its trustworthiness, mainly because of fears of seller opportunism and concerns about the utilization of the associated Internet infrastructure. Moreover, trust creates positive attitudes and perceived behavioral control toward transactions with online retailers, reducing uncertainty and providing expectations for a satisfactory transaction, thus positively influencing behavioral intentions to transact of consumers (Pavlou 2003).

Prior research has heavily studied online shopping intentions. Little is available to shed lights on user’s willingness to supply
personal information in exchange for privileged information. Although the two concepts may share common antecedent variables, their intended focus and the private information involved can be very different. Comparatively the amount and type of private information supplied for online purchases may be far more sensitive than other types of online activities such as information searching.

Some initial findings regarding information disclosure and how it relates to privacy, trust and perceived risk are beginning to emerge. The behavioral intention for not providing information when perceptions of risk and privacy concerns are high is again consistent with expectancy theory in that individuals are motivated to minimize negative outcomes (Dinev and Hart 2006a). In Phelps et al.'s (2001) work, privacy concern is indirectly related to the type of personal information and amount of privacy control through past experience with direct marketing. In the context of online marketing, Yang and Wang's (2009) findings support that privacy concern had a negative effect on information disclosure and a positive effect on protection intention. There is also some support from the literature that users' Internet trust positively affects their willingness to provide personal information in order to purchase products/services and to retrieve privileged information on the Internet (Zosotheos and Kafeza 2009). Collectively some antecedent variables (e.g., privacy concern, trust, and perceived risk) heavily studied in the literature for intention to transact may also have an effect on intention to search for privileged information. Therefore, the following hypotheses are proposed:

Hypothesis 6. Privacy concerns will have a negative effect on intention to transact.

Hypothesis 7. Privacy concerns will have a negative effect on intention to retrieve privileged information.

Hypothesis 8. Perceived risk will have a negative effect on intention to transact.

Hypothesis 9. Perceived risk will have a negative effect on intention to retrieve privileged information.

Hypothesis 10. Trust will have a positive effect on intention to transact.

Hypothesis 11. Trust will have a positive effect on intention to retrieve privileged information.

4.4. The moderating effect of experience

User experience has consistently received attention in the realm of privacy, trust, and security especially in recent works (Gupta and Kim 2007). The relationship between experience and these aforementioned constructs are especially strong in determining behavioral intentions for inexperienced shoppers, because uncertainty in the environment and with the online vendors is likely high in the absence of enough transaction experience (Gefen 2000, McKnight et al., 2002). Consumers with more experience in online transactions are likely to focus less on the trustworthiness of the market or vendor and therefore will care less about factors such as transaction policy, transaction process, and payment security (Kim and Ahn 2007). In addition, experienced shoppers are more familiar with online stores in general, suggesting that the influence of privacy concerns and trust on intentions to transact and retrieve privileged information may be weakened in strength as consumers gain more shopping experience.

Studies are beginning to emerge to consider experience on the interwoven relationships between privacy concerns, trust and other related concepts. For example, while studying privacy concerns, performance expectancy and intention to use location based services between potential and experienced customers, Xu and Gupta (2009) found that there was a significant difference in construct relationships between the two experience groups. Several other studies have also tested the general transaction experience as a moderator of some beliefs on behavioral intentions (Khalifa and Liu 2007, Liang and Huang 1998). Gupta and Kim's work (2007) confirms the role of transaction experience as a moderator on consumer-purchase intention. Moreover, the effect of trust-building factors on intentions to engage in e-commerce activities differs between potential and repeat customers (Gefen et al. 2003b, Kim and Park 2005), suggesting a moderating effect of experience. In addition, as consumers gain more online shopping experience, the effect of generalized privacy concerns will be less important due to a higher level of confidence that also causes them to be more willing to provide personal information during online shopping (Slyke et al. 2006).

When enough experience is accumulated, the impact of privacy concerns and trust on online transactions and information retrieval would decrease. It is worth pointing out that experience as a moderator for behavioral intentions is supported in the literature for both general experience (Xu and Gupta 2009) and experience toward a specific vendor or retailer (Gefen et al. 2003b). Therefore, from a theoretical and practical point of view, there is a reason to expect that the effect of privacy concerns and trust on behavioral intention is moderated by experience. We posit the following hypotheses:

Hypothesis 12a. Experience negatively moderates the relationship between privacy concerns and intention to transact.

Hypothesis 12b. Experience negatively moderates the relationship between privacy concerns and intention to retrieve privileged information.

Hypothesis 12c. Experience negatively moderates the relationship between trust and intention to transact.

Hypothesis 12d. Experience negatively moderates the relationship between trust and intention to retrieve privileged information.

5. Research methodology

5.1. Measurement

This study drew on the existing literature to measure factors in the model. A pre-test of the survey was carried out by two researchers in the field to improve the face validity of the instrument. Forty graduate students participated in the pilot study before the instrument was fully launched to the target population. The result of the pilot study showed that the Cronbach's α value of each construct all exceeded the commonly acceptable minimum of 0.7. All items in the questionnaires used a 5-point Likert scale, with one representing total disagreement and five representing total agreement. Items for Internet literacy, social awareness were adopted from Dinev and Hart (2006b). Items for perceived risk were adapted from Dinev et al. (2006), while items for disposition to trust were adapted from Lee and Turban (2001) and McKnight et al. (2002). Items for trust were based on Cheung and Lee (2001) and Lee and Turban (2001). Privacy concerns, intention to transact and intention to retrieve privileged information were taken from Dinev and Hart (2006a).
There is no single factor that accounts for the severity of common method bias. The result of principal component analysis shows eight factors each with an eigenvalue larger than one. There is no single factor that accounts for the majority of the covariance. In fact, the largest covariance explained by one factor is only 26.88%, indicating that common method bias is not a great concern.

5.2. Data collection

The final survey was administered to a broad sample of individuals in Taiwan, including undergraduate students from four universities, employees from two hospitals, three high-tech companies and two insurance companies, and EMBA students. The average response rate was 50%. A total of 488 questionnaires were received, of which 459 were valid. Table 3 shows the demographic distributions of the sample. 56.2% of respondents were male, and 43.8% were female. 30.9% of respondents were under age 20. 58.2% respondents were between age 20 and 40 and 10.9% of respondents were above age 40. Most of the respondents (74.3%) had 7 years or more of the Internet experience. 43.6% of respondents had not had more than 1 year of online transaction experience, while 56.4% had more than 1 year of online transaction experience. 20.7% of respondents had 5 years or more of online transaction experience. The demographic distribution reveals a diverse sample, comprising a wide range of age and education, with approximately an equal representation of gender. The data was split into two groups based on the respondents’ level of online transaction experience in order to study the moderating effect of user experience. Inexperienced shoppers were those who had not shopped online for more than a year. Experienced shoppers were those who had shopped online for more than a year.

We conducted the Harman’s (1967) one-factor test to assess the severity of common method bias. The result of principal components factor analysis shows eight factors each with an eigenvalue greater than one. There is no single factor that accounts for the majority of the covariance. In fact, the largest covariance explained by one factor is only 26.88%, indicating that common method bias is not a great concern.

6. Data analysis and results

6.1. Measurement model

The partial least squares (PLS) method of structural equation modeling (PLS-Graph 3.0) was used for its ability to handle highly complex predictive models. The reliability of individual items, internal consistency between items and the model’s convergent and discriminant validity were examined to ensure an appropriate measurement model. Table 4 (all shoppers), Table 5 (inexperienced shoppers) and Table 6 (experienced shoppers) show the number of items, mean, standard deviation, composite reliability, average variance extracted (AVE), and square root of the AVE, as well as the correlations between the constructs.

As shown in these tables the composite reliability measures are all greater than 0.80, which is above the recommended value of 0.7 for construct reliability (Bagozzi and Yi 1988). A satisfactory level of convergent validity is maintained since the AVE values of all constructs are above the suggested threshold value of 0.50. Discriminant validity is shown when the square root of each construct’s AVE is larger than its correlations with other constructs (Fornell and Larcker 1981). The square root of each AVE is much larger than its correlations with the other constructs, thereby offering some evidence for discriminant validity.

6.2. Structural model assessment and hypotheses testing

The structural model is shown in Fig. 2 for the whole sample (all valid responses included). The statistical significance (p < .001) for the path coefficients supports most of the hypotheses (H2–H11). Internet literacy impacts privacy concerns with a path coefficient of 0.14 at the 0.01 level of significance. This is in the opposite direction of the first hypothesis. Consistent with the second hypothesis, social awareness is positively correlated with privacy concerns, with a path coefficient of 0.20 (p < .001). Hypothesis H2 was supported.

Support was found for the remaining hypotheses: Perceived risk was positively related to privacy concerns, with a path coefficient of 0.44 at the 0.001 level of significance. Hypothesis H3 was supported. Perceived risk was negatively correlated with trust, with a path coefficient of –0.45. Hypothesis H4 was supported. Support was also found for H5, with disposition to trust affecting trust, with a path coefficient of 0.17.

The paths from privacy concerns to intention to transact (H6) and intention to retrieve privileged information (H7) were negative and statistically significant, with path coefficients of –0.15,
ents and construct relationships remained the same between the two models. The purpose is to provide a comparison for the effects of the two related but fundamentally different dependent variables (intention to transact and intention to retrieve privileged information). The two-dependent-variable model reported in this article explains a larger amount of variance (58%) for the intention to transact variable, as opposed to only 42% in the one-dependent-variable model. This significant improvement provides some beginning evidence for the separation of the two dependent variables, in favor of the final model reported here in this study.

Table 7 shows the direct, indirect, and total effect of each construct on the two dependent variables. The indirect effect of Internet literacy (−0.042 vs. −0.039), social awareness (−0.060 vs. −0.056) and disposition to trust (0.065 vs. 0.060) on intention to transact is similar to their effect on intention to retrieve privileged information. The effect of trust on the two intention variables (0.380 vs. 0.350) was slightly stronger than the effect of privacy concerns on the same intention variables (−0.300 vs. −0.280). Moreover, the direct effect of perceived risk on intention to transact (−0.260) is smaller than all its indirect effects combined (−0.28 = −0.30 + −0.45 × 0.38 = −0.303), while the same thing is also true for its indirect effects on intention to retrieve privileged information (direct effect: −0.23 vs. indirect effects: −0.45 × 0.35 + 0.44 × 0.28 = −0.281). Collectively the direct effects from perceived risk to the two intention variables are smaller than their respective indirect effects. The magnitude of difference, however, is not large, suggesting that both types of effects are relevant.

As shown in Fig. 3 (inexperienced shoppers) and Fig. 4 (experienced shoppers), inexperienced shoppers’ privacy concerns were influenced by their Internet literacy and social awareness, but the same is not confirmed for the experienced shoppers. Disposition seems to have an effect on trust for inexperienced shoppers only. Furthermore, both samples (inexperienced versus experienced) show that privacy concerns, risk and trust influence intention to transact and retrieve privileged information, but the relationships are significantly stronger for inexperienced shoppers.
than for experienced shoppers. These constructs explained 56% of the variance of intention to transact and 42% of the variance of intention to retrieve privileged information for inexperienced shoppers. Moreover, 51% of the variance of intention to transact and 42% of the variance of intention to retrieve privileged information for experienced shoppers. The explained variance for privacy concerns was 30% for inexperienced shoppers and 34% for experienced shoppers. The explained variance of trust was above 30% for both groups.

6.3. Moderation analysis

A moderation analysis was conducted to test the validity of the moderation hypotheses (H12a to H12d). The moderating effect is tested using the equation developed in Chin (2009). The results in Table 8 show that online transaction experience moderates the effect of privacy concerns on intention to transact ($\Delta\beta = -0.24$, $p = 0.01$) and intention to retrieve privileged information ($\Delta\beta = -0.16$, $p = 0.01$) and trust on intention to transact ($\Delta\beta = 0.13$, $p = 0.01$) and intention to retrieve privileged information ($\Delta\beta = 0.15$, $p = 0.05$). Thus, H12a to H12d were supported.

The data were split at median of the experience variable (years of shopping experience), resulting in two sets of sub-samples: inexperienced shoppers (IS) and experienced shoppers (ES). Inexperienced customers were those who had not shopped online for more than a year. Experienced customers were those who had shopped online for more than a year. Fig. 5 shows a graphical representation of the moderation effects on pairs of constructs. Transaction experience significantly moderates the effect of privacy concerns on intention to transact and retrieve privileged information. With an increased level of transaction experience, the influence of privacy concerns on transaction and information retrieval intentions reduces strength. Another interesting finding is that the influence of trust follows the same pattern of weakening as transaction experience increases.

7. Discussion

This study is designed to build an integrated model from existing theories to examine the effect of privacy, trust, risk and related factors on two activities: online transactions and online privileged information searching. The difference in the requirements for privacy and the accuracy of the provided personal information between the two activities both have an effect on the privacy control opportunities that a consumer can exercise. Additionally, research regarding privileged information searching is largely lacking, adding much complexity to our understanding of the perception-versus-behavior relationship for these online activities. This study offers some empirical evidence of privileged information searching, its antecedents and its relationship with online transactions.

Findings in the present study show that Internet literacy affects privacy concerns, but in the opposite sign as postulated in H1. Generally as the Internet literacy goes up, people are less concerned of their privacy due to their familiarity with the techniques they can exercise to better control their personal information. This
assumption perhaps only works to a certain extent as most Internet users are non-techies and many rely on automatic procedures (e.g., antivirus scans) for their protection. Such an automatic protection does not go well when an individual unknowingly passes their private information to a third party during online activities, such as games, information searches and online registrations. As an individual grows more aware of the many ways that a third party can collect user information, they may become more concerned of how their personal information is transmitted and used by a total stranger.

Social awareness was positively related to privacy concerns (H2), a finding consistent with Dinev and Hart (2006b). This implies that individuals who are aware of the social and political processes tend to exhibit more Internet privacy concerns. Perceived risk was found in the present study to be the most significant determinant of privacy concerns (H3) and trust (H4). This is an important finding that has both theoretical and empirical significance. Perceived risk in this study exhibits a large explanatory power on privacy concerns and trust. Risks derived from technology uncertainty include theft of credit card information, breach of private information, and stealing of personal information by hackers and scam artists (Yousafzai et al. 2003). A few techniques that can partially alleviate consumer’s risk concerns include encrypted transactions, layers of authentication procedure, anti-phishing schemes, and privacy seals and disclosures. Additionally, third-party trust certifications (such as better business bureau, or BBB) and alliance with larger trusted organizations (such as small vendors who open a “market” storefront at Amazon.com) are also ways to building consumer trust. However, consumers cannot physically examine their products before purchases, and they worry about the divulgence of their personal information and credit card number through the transaction with the online retailers. Examples of opportunistic behavior in e-vendor by a vendor include product/service misrepresentation, false identity demonstration, denunciation of warranties and private information leak (Yousafzai et al. 2003). As expected, the consumers’ perceived risk exhibits the most significant impact on privacy concerns and Internet trust in e-commerce.

Disposition to trust was positively related to trust (H5). This is also consistent with previous studies (Dinev et al. 2006, Teo and Liu 2007). Customers who are trusting in general will also likely to trust vendors on the Internet than those who are not. Ideally disposition to trust is the main source that leads to the trust behavior, but our study shows a partial support to this assumption. Only the more inexperienced shoppers were found to have a positive and statistically significant relationship between trust and disposition to trust.

The results of this study show that perceived risk, privacy concerns and Internet trust were significant predictors for the intention to transact and retrieve privileged information. Therefore, H6 to H11 are supported. The significance of this finding lies in that prior studies (e.g., Dinev and Hart 2006a, Dinev et al. 2006, Pavlou 2003, Pavlou and Gefen 2004) incorporated privacy concerns, risk and trust as predictors of intention to conduct online transactions, but the present study goes one step further to examine both transaction and information searching activities in an integrated model. The variance explained by the two activity variables and the

---

**Table 8**

Results of the moderating effect of experience.

<table>
<thead>
<tr>
<th>H12a</th>
<th>Privacy concerns → intention to transact</th>
<th>IS&lt;sup&gt;a&lt;/sup&gt;</th>
<th>SE</th>
<th>β</th>
<th>t-Value</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>0.0</td>
<td>0.07</td>
<td>0.91</td>
<td>0.24</td>
<td>-2.80**</td>
</tr>
<tr>
<td>H12b</td>
<td>Privacy concerns → intention to retrieve privileged information</td>
<td>0.05</td>
<td>0.05</td>
<td>0.66</td>
<td>-0.16</td>
<td>-2.58**</td>
</tr>
<tr>
<td>H12c</td>
<td>Trust → intention to transact</td>
<td>0.04</td>
<td>0.04</td>
<td>0.5</td>
<td>0.13</td>
<td>2.60**</td>
</tr>
<tr>
<td>H12d</td>
<td>Trust → intention to retrieve privileged information</td>
<td>0.04</td>
<td>0.05</td>
<td>0.64</td>
<td>0.15</td>
<td>2.48**</td>
</tr>
</tbody>
</table>

---

<sup>a</sup> IS: inexperienced shoppers, ES: experienced shoppers.

* P < 0.05.

** P < 0.01.

*** P < 0.001.

---

Fig. 5. Graph of moderating effect of experience on inexperienced shoppers and experienced shoppers.
moderate $R^2$ both imply that the two variables are distinct variables that share similar antecedents.

Findings from the present study also suggest that Internet customers with higher social awareness, higher Internet literacy and higher perceived risk tended to be the ones with the highest privacy concerns. These Internet customers were politically and socially engaged and had a high level of social awareness. Therefore, it is possible that they were able to easily grasp the seriousness of privacy problems, the core vulnerabilities and the insecurities of the Internet. This argument is consistent with Han and Maclaurin’s (2002) findings about eroding customer confidence in information privacy concerns.

We examined direct, indirect, and total effects of variables that predict the two intention variables. Perceived risk directly influenced both intention to transact and intention to retrieve privileged information. It also had an effect on the two variables indirectly through privacy concerns and trust. Some prior studies support the direct effect of perceived risk on intentions (Nicolaiou and McKnight 2006, Pavlou 2003). However, we found that perceived risk had a stronger indirect effect on the two intention variables (−0.303 vs. −0.281) through privacy concerns and trust than its direct effect on the same intention variables (−0.260 vs. −0.230). Moreover, it had a stronger indirect effect through trust on the two intention variables (−0.171 vs. −0.158) than its indirect effect through privacy concerns (−0.132 vs. −0.123). According to the path coefficients, trust exhibited a strong direct effect on intention to transact (0.380). This supports prior studies in that trusting beliefs directly influence intentions. Our findings also show that the same is true for its effect on intention to retrieve privileged information, although with a slightly smaller path coefficient (0.350). In addition, perceived risk exhibited the strongest total effect on intention to transact (−0.563). This finding is in line with prior studies, in which both perceived risk and trust were significant predictors of behavioral intentions. The role of these predictors in their relationship with privileged information searching is also empirically confirmed, an area that has not received much attention in the literature.

8. Implications

Our findings suggest that respondents are concerned about their privacy as they became more Internet literate. This may be due to in part that the more knowledgeable they are regarding the possible privacy threats on the Internet, the more they fear about not being able to have a full control of their own personal information once it leaves their computers. One way to alleviate this concern is to offer some form of privacy assurance, such as privacy seal and privacy policy. However, many anecdotal stories have portrayed Internet users’ lack of interest in going through legal or lengthy statements in a privacy policy. In addition to a centralized lengthy privacy policy, companies are recommended to offer immediate assurance, where a simple privacy assurance statement is displayed next to the area that asks for private or personal information.

In addition, high social awareness only leads to high privacy concern for the inexperienced shoppers, an effect very weak for experienced shoppers. The magnitudes of the path coefficients for both types of shoppers are rather low, indicating that social awareness merely had a marginal effect on one’s privacy concern. Since social awareness is a factor that individual vendors find it difficult to influence, few opportunities are available for online merchants. Recently cross-linking to privacy education sites from a vendor’s main web site is an emerging practice. Despite the benefits of user privacy education and demonstration of the company’s commitment to privacy protection, such practice has not received enough research for its effect on social awareness and privacy concern. More can be explored in future studies.

One fundamental difference between the two dependent variables is that users may be able to exercise a certain level of privacy control in order to retrieve privileged information. Our findings show that the effects from the immediate antecedent variables are rather similar for the two dependent variables, indicating that the two variables may share some characteristics that are related to an individual’s perception on privacy, risk and trust. This not only extends the possibility of applying antecedent variables verified in existing studies for the intention to transact variable to intention to retrieve privileged information, but it also suggests that traditional techniques (e.g., privacy seal and security certificates) to alleviate privacy concerns, reduce perceived risks and engender trust may be applicable to intention to retrieve privileged information. If it is not absolutely necessary, e-marketers are recommended to reduce their request for more sensitive information until a relationship has been established with the customers. This will provide a significant payoff in the long run with regard to elicitation of user information (Metzger 2007).

The overall sample was split into two experience groups to study the moderating effect of user experience and how the two groups differ in construct relationships. Privacy concerns and trust of inexperienced consumers were affected primarily by their individual characteristics (such as Internet literacy, social awareness, and trusting disposition), while the same was not true for the experienced consumers. In addition, the effect of privacy concerns, perceived risk and trust on the two dependent variables is weaker for the more experienced shoppers. Since experienced shoppers are those who have already engaged themselves in online shopping, the diminishing effect of privacy, risk and trust may signify that their longer history of shopping experience perhaps overshadows fundamental worries. This at least gives vendors some leeway to pursue other forms (e.g., incentives that are applied to return consumers) of user engagement at their e-commerce website. However, this is not to say that mechanisms that affect the three immediate antecedent variables (i.e., privacy concerns, etc.) are not useful. Internet marketers are still recommended to adopt several trust-building mechanisms to enhance favorable consumer perceptions, especially for inexperienced consumers. Even with experienced shoppers, enhancing trust leads to a higher level of loyalty with the vendor and repurchase intentions (Gefen 2002).

Internet marketers are recommended to continue researching practical ways to alleviate privacy concerns, privacy risk and increase trust by assuring safety of consumers’ personal information and engaging in privacy assurance techniques, including accreditation by reputable institutions (Pavlou et al. 2007) and participation in privacy certification programs along with making their privacy policy easy to comprehend. As mentioned in preceding paragraphs simple privacy pledges next to where private information is required may calm privacy and risk concerns. A succinct and well-presented privacy policy such as “we will never sell your private information” may reduce privacy and risk concerns and increase trust with the Internet marketers (Featherman and Pavlou 2003). Third-party assurance seals including security (e.g., Verisign, WebTrust), privacy (e.g., TRUSTe, BBBOnline Privacy), and business integrity (e.g., BBBOnline Reliability, BizRate.com certified), security features (SET, SSL, locks, etc.), and privacy policy statements on their websites (Belanger et al. 2002, Kim et al. 2008, Schoder and Yin 2000) are among the techniques that an online vendor may start to offer. In addition, group effect is likely to influence customers’ purchase decision (Witt and Bruce 1970, Tauber 1972). It may also be used as a way to soothe privacy concerns and perceived risks by fostering a sense of trust. Displaying transaction statistics, user experience and
Several theoretical and practical contributions are possible from this research. An Academy of Management Review editor once said “[T]heoretical insights come from demonstrating how the addition of a new variable significantly alters our understanding of the phenomena by reorganizing our causal maps” (Whetten 1989, p. 493). Results from our study are in line with this comment. First, this study identifies variations of relationships between privacy concerns, risks, trust and their antecedents based on users’ preexisting experience with online transactions. Many previous studies look at risk or trust by assuming user experience either stays constant or as an antecedent that exerts influence on a handful of variables. The result from the present study shows that the significant moderating effect of user experience had an impact on construct relationship and the strength of paths. Second, two dependent variables (intention to transaction and intention to retrieve privileged information) studied in the integrated model allows us to examine the effect of antecedents simultaneously when both dependent variables are present. Most prior research focuses primarily on how privacy and trust are related to an individual’s intention to conduct online transactions. Very little is known about a consumer’s intention to supply personal information in exchange for certain privileged information online. The inclusion of privileged information search in our integrated model introduces a new construct and a new set of relationships with existing constructs, which also leads to theoretical contributions to the literature. Third, unlike online shopping, where certain private information is required to be accurate and verified, privileged information searching activities that require sending of personal information frequently do not strictly require accuracy of the personal information. Therefore, opportunities abound for an individual to exercise different techniques (e.g., falsification and omission) to control what personal information is to be delivered to the merchant. Our study offers a step further to examine how the antecedents affect these two similar but fundamentally different Internet activities. Fourth, this study confirms the role of antecedents of privacy concerns and trust, as well as the latter two as the antecedents of the two activities variables. Fifth, the theoretical model that simultaneously integrates layers of factors based on several existing studies offers contributions in its own right and also extends our understanding of how individuals’ intrinsic measures of privacy, trust and risk affect their intention for the outcome activities. Finally, this study is non-US based. As such, it provides some level of generalizability beyond the US sample, thus expanding the applicability of the research model.

9. Conclusion

Prior studies have primarily focused on only privacy concerns relating to online transactions, rather than other forms of online activities. In the foreseeable future, information sharing and cloud-based computing (e.g., Google and Amazon web services) may continue to spark different forms of trust and privacy issues. An individual’s information (private or not) will likely to be available online for the person or interested parties. Further studies into the inter-twined privacy and trust relationships with transactional and non-transactional activities may be a starting point to fill the gap.

Privacy and trust have been identified as key to e-commerce success. This paper provides several insights into the role of Internet literacy, social awareness, perceived risk and disposition to trust on the issue of privacy concerns and trust in e-commerce. This study also highlights the importance of using privacy concerns and trust as two distinct concepts. This study examines how the relative importance of these two constructs and of their antecedents differs between inexperienced shoppers and experienced ones. Findings of this study identified important differences between the determinants of transaction intentions for inexperienced shoppers vis-à-vis experienced shoppers. The results in this study thus have significant implications for both the theory and practice of e-commerce.

Future research may explore the role of extrinsic factors in conjunction with an individual intrinsic assessments studied in the present research. In light of the globalization of Internet, it is also interesting to extend this study to include societal and cultural factors. We plan to extend this study to other countries in order to explore how cultural affects the construct relationships. Since personality traits such as social awareness and trusting disposition are built over a lifelong experience, changes on one’s privacy concerns and trust are likely due to multiple sources of influence (including culture and societal elements) that may happen at different points in time.

Appendix A. Survey questionnaire and factor loadings

<table>
<thead>
<tr>
<th>Construct</th>
<th>Item</th>
<th>Loading</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet literacy</td>
<td>Identify and delete a program which you consider intrusive (spyware) and which was installed through the Internet without your knowledge and permission</td>
<td>0.73</td>
</tr>
<tr>
<td>Social awareness</td>
<td>I am interested in reading political commentaries or watching them on TV</td>
<td>0.70</td>
</tr>
<tr>
<td>Perceived risk</td>
<td>Personal information submitted could be misused</td>
<td>0.93</td>
</tr>
<tr>
<td>Disposition to trust</td>
<td>I am a trusting person</td>
<td>0.87</td>
</tr>
<tr>
<td></td>
<td>I trust people in general</td>
<td>0.90</td>
</tr>
<tr>
<td></td>
<td>I think most people can be trusted</td>
<td>0.85</td>
</tr>
</tbody>
</table>

(continued on next page)
<table>
<thead>
<tr>
<th>Construct</th>
<th>Item</th>
<th>Loading</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy concerns</td>
<td>I am concerned that the information I submit on the Internet could be misused</td>
<td>0.87</td>
</tr>
<tr>
<td></td>
<td>I am concerned that a person can find private information about me on the Internet</td>
<td>0.82</td>
</tr>
<tr>
<td></td>
<td>I am concerned about submitting information on the Internet because of what others might do with it</td>
<td>0.85</td>
</tr>
<tr>
<td></td>
<td>I am concerned about submitting information on the Internet because it could be used in a way I did not foresee</td>
<td>0.85</td>
</tr>
<tr>
<td>Trust</td>
<td>Internet websites are safe environments in which to exchange information with others</td>
<td>0.85</td>
</tr>
<tr>
<td></td>
<td>Internet websites are reliable environments in which to conduct business transactions</td>
<td>0.86</td>
</tr>
<tr>
<td></td>
<td>Internet websites handle personal information submitted by users in a competent fashion</td>
<td>0.83</td>
</tr>
<tr>
<td>Intention to transact</td>
<td>Purchase goods (e.g., books, CDs) or services (e.g., airline tickets, hotel reservations) from Web sites that require me to submit accurate and identifiable information (i.e., credit card information)</td>
<td>0.92</td>
</tr>
<tr>
<td></td>
<td>Conduct sales transactions at e-commerce sites that require me to provide credit card information (e.g., using sites for purchasing goods or software)</td>
<td>0.94</td>
</tr>
<tr>
<td>Intention to retrieve privileged information</td>
<td>Retrieve information from Web sites that require me to submit accurate and identifiable registration information (e.g., using sites that provide personalized stock quotes, insurance rates, or loan rates)</td>
<td>0.89</td>
</tr>
<tr>
<td></td>
<td>Retrieve highly personal or private information</td>
<td>0.88</td>
</tr>
</tbody>
</table>

References


Fornell, C., and Larcker, D. F. Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18, 1, 1981, 39–50.


