Decision Support Systems 57 (2014) 343–354

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns

Yuan Li *

Division of Business, Mathematics and Sciences, Columbia College, Columbia, SC 29203, USA

ARTICLE INFO

Article history:
Received 2 February 2012
Received in revised form 3 September 2013
Accepted 27 September 2013
Available online 5 October 2013

Keywords:
Information privacy concerns
Disposition to privacy
Website reputation
Website familiarity

ABSTRACT

This study examines the impact of disposition to privacy, perceived reputation of a website, and personal familiarity with the website on a person's privacy concerns about the website. It also analyzes the key attributes of disposition to privacy and its antecedents. Using a survey, the study finds the direct impact of disposition to privacy, website reputation, and personal familiarity on website-specific privacy concerns. The impact of privacy experience on disposition to privacy is also confirmed. The moderating effects of website reputation and personal familiarity on disposition to privacy are not supported, suggesting that the three antecedents exert their impact on privacy concerns independently. The study extends the information privacy literature through the analysis of the roles of contextual factors (reputation and familiarity) in the relationship between disposition to privacy and website-specific privacy concerns. It also moves forward studies on individual disposition to privacy, calling for more attention to this critical concept.

1. Introduction

Privacy is an important social issue affecting all individuals, as the lack of privacy prevents people from disclosing themselves in social interactions. To date, scholars have studied privacy from different perspectives and have recognized approaches to protecting privacy [44,61,68]. In the e-commerce literature, research has focused on online information privacy from the consumer's perspective due to the impact of the Internet and the web on consumer information privacy. A large number of factors that influence consumer privacy concerns and behaviors have been studied [10,38,50,61]. Among those factors, disposition to privacy, representing a person's general "desire for privacy" [10,61], plays important roles in determining privacy behaviors on the Internet [55,69,70].

Despite the theoretical and practical importance of the concept [4,33,66], disposition to privacy has received limited attention in the e-commerce literature. Only a few studies examined its effect in the e-commerce domain [55,69,70], but little is known about how the effect may be influenced by contextual factors in a certain circumstance, such as on an e-commerce website. Fundamental to this issue is the recognition of the key attributes of disposition to privacy, which have remained elusive in the literature. Addressing these issues is critical to the development of knowledge in the area.

In this study, we examine the impact of disposition to privacy on website-specific privacy concerns under the influence of two contextual factors: perceived reputation of a website and personal familiarity with the website. Specifically, we aim at answering three research questions. 1) *What is the nature of disposition to privacy, and how is it related to a person's privacy concerns about a website*? Due to the limited studies on disposition to privacy in the e-commerce literature, we conduct a review on several important theories in the sociological and psychological literature to clarify the concept. 2) *How do the contextual factors, such as the reputation of a website and personal familiarity with the website, influence the relationship between disposition to privacy and website-specific privacy concerns*? We notice that several contextual factors, such as the effectiveness of privacy policies and the effectiveness of industry self-regulation, were studied for their impact on website-specific privacy concerns [69]. Nevertheless, scholars show that the readability of privacy policies is declining due to the length of the policies and complexity in contents, and approximately half of the consumers in the United States do not have the education level needed to understand about half of the online privacy notices [47]. In addition, few consumers ever notice or read the policies [45,49]. Therefore, we investigate the influence of other contextual factors on information privacy to extend the literature. 3) *What are the antecedents to disposition to privacy*? We notice a paucity of empirical studies on the antecedents to disposition to privacy, so we explore several factors that may explain its development.

The structure of the paper is as follows. In Section 2, the literature review is presented, based on which disposition to privacy is examined and its impact on website-specific privacy concerns is explored. In Section 3, the research model is presented and the hypotheses are developed. Research method and data collection process are reported

* Tel.: +1 803 786 3678; fax: +1 803 786 3804.
E-mail address: yli@columbiasc.edu.

0167-9236/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.dss.2013.09.018

in Section 4, and data analysis and results are reported in Section 5. Finally, contributions, implications, and limitations of the study are discussed in Section 6.

2. Literature review

A number of theories were developed to explain individual disposition to privacy [4,33,43,66]. These theories suggest that disposition to privacy is the outcome of a person's social interactions with others that enables the person to achieve expected status such as personal autonomy or to deter unexpected status such as dehumanization [44]. A few studies in the e-commerce literature adopted this concept. For example, Yao et al. [70] found the impact of disposition to privacy on a person's privacy concerns about the Internet, and Xu et al. [69] found the impact of disposition to privacy on website-specific privacy concerns. A similar concept, need for privacy, was examined for its moderating effect in website use [55]. As studies on disposition to privacy are still limited in the e-commerce literature, efforts are needed to better understand this concept and to examine its effect on website use. We review several popular theories on privacy to learn this concept and to examine its impact on website-specific privacy concerns.

2.1. Disposition to privacy: Toward a conceptual clarity

As mentioned above, disposition to privacy stands for a person's general desire or need for privacy across contexts, which distinguishes it from other learned dispositions within certain contexts, such as situational privacy concerns [37,69]. In other words, disposition to privacy represents a person's general attitude toward privacy. This concept has been theorized from various perspectives that focused on different issues [4,61]. Of the many theories proposed, Westin's [65,66] and Altman's [3,4] theories are perhaps the most influential [43,44]. Laufer and Wolfe's theory [33] also provides a profound basis for e-commerce research [17,69]. We focus on these three theories in the review.

2.1.1. Westin's theory

Westin's theory [65,66] is particularly relevant to e-commerce research due to its emphasis on information privacy [43]. He defines privacy as the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others [66]. He posits that people have a need for privacy that, in concert with the needs for disclosure such as socializing [25,66], helps them to adjust emotionally to daily life with others. The benefits or functions of privacy include emotional release (release from the tensions of social life), personal autonomy (desires to avoid being manipulated, dominated, or exposed by others), self-evaluation (integrating experience into meaningful patterns and exerting individuality), and limited and protected communication (setting interpersonal boundaries and sharing personal information with trusted others) [43,65]. From the e-commerce perspective, these privacy functions help reduce consumers' anxiety about the Internet and enhance their abilities to control information disclosure for expected outcomes.

Westin proposes four means (called *States*) to achieving privacy: solitude, intimacy, anonymity, and reserve. Solitude is being free from observation by others, a status also known as exclusion or withholding. Intimacy refers to small group seclusion for group members to achieve a close, relaxed, and frank relationship. Anonymity refers to freedom from identification and surveillance in public places, which is a key area of research in the e-commerce literature [55]. Finally, reserve is based on the desire to limit information disclosures to others, and it requires others to recognize and respect that desire. If such desire is violated by others through the process known as peer's disclosure [15], privacy is invaded. Of these means to privacy, anonymity and reserve have particular importance to e-commerce, as they relate to the collection and secondary use of personal information by e-commerce websites.

A well-known contribution of Westin and his colleagues is the classification of individuals into three categories based on their extent of privacy dispositions, including privacy fundamentalists, privacy unconcerned, and privacy pragmatists [66]. Privacy fundamentalists are high-privacy oriented individuals who reject consumer-benefit or societal-protection claims for data use and search legal-regulatory privacy measures. The privacy unconcerned belongs to the limited-privacy camp who would be ready to supply personal information to businesses and governments. Between these two camps are privacy pragmatists, who like the balanced-privacy position and make information disclosure decisions based on the privacy calculus [61]. Recognizing the distinct privacy dispositions of individuals help businesses to design appropriate privacy policies and incentive schemes to elicit information from customers [6,7,26,35].

Other aspects of Westin's theory are also noteworthy [4,43]. For example, he suggests that people seek a balance between openness (e.g., disclosure) and closeness (e.g., non-disclosure): to be with others and to be away from others at different times. He notes that too much or too little separation from others is an undesirable state of affairs, suggesting a non-monotonic, dialectic approach to privacy. This approach was followed by others in further theorization [4,52].

2.1.2. Altman's theory

Altman's theory [3,4] constitutes another important foundation for privacy research [43]. Similar to Westin, Altman conceptualizes privacy as a control mechanism, defining it as the selective control of access to the self or to one's group. This definition demands a multi-level research on privacy at and across individual and group levels [10]. The main propositions of Altman's theory include: units of analysis varying from individuals to groups, the dialectic nature of privacy, the non-monotonic nature of privacy, privacy as a boundary regulation process, and privacy as a bidirectional process [4]. In terms of the units of analysis, Altman suggests that privacy is an interpersonal event involving linkages between persons or groups. The solitude and anonymity states of privacy (see Westin's theory), for example, involve an individual seeking privacy from others, while the intimacy and reserve states involve a group of people seeking privacy from other people or groups. For the dialectic nature of privacy, Altman states that social interaction is a continuing dialectic between forces driving people to come together and to move apart, as there are times when people want to be alone and times when others are sought out. Therefore, privacy targets a momentary, ideal level of interpersonal contact, and "ideal" privacy is a position on the continuum between isolation and intrusion. The dialectic nature of privacy determines that it is non-monotonic: neither too much nor too little privacy is satisfactory, and people seek an optimal level of privacy in social interactions. In other words, even the privacy fundamentalists may choose to release personal information for certain benefits [26], and the privacy unconcerned may prefer certain degree of solitude or anonymity if necessary.

An important contribution of Altman's theory is the depiction of privacy as an interpersonal boundary control process. He suggests that privacy involves a temporal, dynamic process of control over interpersonal boundary that changes how open one is in response to changes in one's internal states (e.g., the need for solitude and exclusion) and external conditions (e.g., the need for anonymity and protected communication). This process helps one to pace the interactions with others [43]. Other studies extended the boundary control mechanism in various privacy contexts [33,52,53,69]. Altman also depicts the distinctions between desired and actual levels of privacy, suggesting that a balance is achieved when desired privacy matches actual privacy [4]. This differs from earlier privacy theories that over-emphasize solitude and exclusion, and it inspires further research on procedural fairness to protect privacy [17].

In addition, Altman summarizes several mechanisms for achieving desired privacy, such as verbal and nonverbal behaviors, environmental behaviors (e.g., the physical condition), and cultural norms and customs

[4]. Other mechanisms are recognized in the e-commerce literature, such as word-of-mouth [62]. How successful these mechanisms help to achieve desired privacy would influence the privacy disposition of a person. For instance, culture is found to influence the general privacy beliefs in a society [11].

2.1.3. Laufer and Wolfe's theory

Laufer and Wolfe [33] recognize several cognitive, social, and biological bases of privacy. They suggest that because of the limited cognitive abilities to fully know oneself and others, information becomes unavailable to some people, setting the stage for attempts to control it. Such an individual or collective awareness of the unknown is even more severe due to the social structure that separates people from each other. Thus, the conscious and unconscious fears of undisclosed/hidden information are generic to personality and social structure, predicting a need for preserving privacy. Human physiology and biology also place limits on continuous interaction among people, providing a basis for the development of needs and desires for managing social interaction and governing the privacy.

Laufer and Wolfe propose a developmental theory of privacy that relates an individual's knowledge of privacy to his or her growth and life over time within particular socio-historical situations [33]. They categorize the elements of privacy situations into three dimensions: self-ego, environmental, and interpersonal. The self-ego dimension focuses on the developmental experience of being capable of functioning independently to achieve individuation and autonomy, such as choosing to be alone. The environmental dimension contains the elements that set the boundaries of personal experience, including culture, social arrangements, physical settings, and the stage of the life cycle (e.g., childhood versus adulthood). The interpersonal dimension consists of elements of social interactions, and two main elements are emphasized: information management (e.g., what to share) and interaction management (e.g., to whom to share). Inability to manage either or both may cause privacy concerns. The developmental process of individual privacy and the three categories of situational elements constitute the main contributions of Laufer and Wolfe's theory. They also suggest that people will perform a calculus of behavior to balance the positive and negative consequences of social interactions, a behavior typically known as privacy calculus in the e-commerce literature [61].

2.1.4. Summary

Based on the above review, we summarize several key attributes of disposition to privacy in Table 1; their implications for hypotheses development are also listed in the table. We notice that disposition to privacy is the desired control of personal information in the social interaction with others. It is idiosyncratic, as its development is influenced by a combination of individual and social-environmental factors. It is instrumental, as it regulates communications to maintain healthy inter-personal relationships. Such disposition can be fulfilled by a number of means such as solitude, intimacy, anonymity, and reserve. Its impact is, however, dialectic and contingent upon factors such as actual level of privacy and need for disclosure. These attributes help to study the relationship between disposition to privacy and website-specific privacy concerns and also its relationship with contextual factors.

It should be noted that privacy has been conceptualized from various perspectives, including privacy as a human right, privacy as a commodity, privacy as a state, and privacy as control [61]. Our view of privacy as information control, built upon the above theories, pertains to the e-commerce research and is popular in the literature [10]. Potential limitations of this view are discussed in Section 6.3.

2.2. Privacy concerns about a website

Privacy concerns about a website are a type of situation-specific concerns [69]. They deal with the privacy perceptions about a specific website rather than the general e-commerce environment, and they occur when the actual privacy on the website does not match the expected privacy by the customer. Studying this type of privacy concerns helps online firms to improve their privacy practices [9,51]. To date, a number of factors were found to have an impact on website-specific privacy concerns, such as the reputation of a website [5,18]; privacy policy and rewards [5]; privacy assurance [34]; information sensitivity and relevance [41]; trust, website informativeness, and website social presence [51]; and also perceived privacy control, privacy risk, and disposition to privacy [69]. Many of the factors reside at the organizational level, which can be interpreted from the agency theory perspective since websites are the agents that collect and use customer information for service and transactions [51]. Less is known about the direct impact of individual-level factors on website-specific privacy concerns. A potential reason is that many individual-level factors, such as demographic attributes, are linked to the general privacy concerns rather than the situational concerns [38].

Disposition to privacy is an individual factor that may influence website-specific privacy concerns. Xu et al. [69] explain, from the communication boundary management perspective [52,53], that an individual who has a higher level of disposition to privacy will be more likely to perceive the boundary penetration (e.g., information collection from a website) as intrusion and thus will be more concerned about his or her privacy. We argue, in line with the above review and especially the summary in Table 1, that disposition to privacy play more roles in determining website-specific privacy concerns: people differ in their dispositions to privacy, which determines that the fear to lose the control of personal information during the interaction with a website may differ, so that their privacy concerns about a website may vary. We elaborate the rationales in Section 3.1.

Extending past research [69], we study two contextual factors that may influence website-specific privacy concerns: the reputation of a website and personal familiarity with the website. Website reputation was shown to have a direct impact on privacy concerns [5,18], although its relationship with privacy disposition was not analyzed. The other contextual factor, personal familiarity with the website [21], refers to the overall understanding of a website based on a person's previous interactions, experiences, and learning of what the website does with users' private information [7]. It deals with the socio-relations between a person and a website, which provides first-hand information on the privacy practice of the website. Although the moderating effect of website familiarity was analyzed in privacy literature [64], we argue that it may also have a direct impact on privacy concerns.

Consistent with the Antecedent-Privacy Concerns-Outcome (or APCO) model of information privacy [61], we examine the impact of website-specific privacy concerns on behavioral intention to use the website. In addition, since the privacy calculus [61] indicates that online consumer behavior is influenced by not only privacy concerns but also benefit beliefs, we include perceived benefit as a control variable to verify the relative importance of privacy concerns [31,71]. Furthermore, we test the impact of privacy experience and demographic factors on disposition to privacy to address limited empirical studies on the antecedents to this construct. The research model and hypotheses are developed in the next section.

3. Research model and hypotheses

Fig. 1 shows the research model. At the core of the model are the impacts of disposition to privacy, website reputation, and website familiarity on website-specific privacy concerns and also the relationship among the three antecedents (Hypotheses 1–5). An antecedent to disposition to privacy, privacy experience, is studied in Hypothesis 6. The impact of website-specific privacy concerns on behavioral intention to use the website is studied in Hypotheses 7. Several control variables such as demographic factors and perceived benefits are also included. The hypotheses are developed as follows.

Table 1
Key attributes of disposition to privacy.

Attributes of disposition to privacy	Supporting literature	Implications for hypotheses development
Desired control of personal information	Disposition to privacy is not merely the exclusion from others, but the desired control of access to personal information by others [4,66]. It is an expectation for privacy.	Hypothesis 1
Inter-personal	Disposition to privacy is not purely an individual phenomenon but comes across levels from individuals to societies [10], and can be better analyzed through social interactions with others [4,43,65]. It is an interpersonal boundary control process that targets an ideal balance between openness and closeness [4].	Hypotheses 1, 4 and 5
Idiosyncratic	People differ in the extent of disposition to privacy, which categorizes them into privacy fundamentalists, privacy pragmatists, and privacy unconcerned [66].	Hypothesis 1
Developmental	The extent of disposition to privacy is subject to the impacts of a number of individual and socio-environmental factors [4]. A typical factor is the developmental stage of a person; others include cultural background and environmental conditions [33].	Hypothesis 6
Instrumental	Disposition to privacy determines the extent to which a person gets involved in self-determined (i.e., personal autonomy) social interactions with others based on emotional release and limited or protected communication [66].	Hypothesis 7
Equifinal	Desired privacy can be achieved (i.e., transformed into actual privacy) by means of solitude, intimacy, anonymity, and reserve [66]; verbal and nonverbal behaviors, environmental behaviors, cultural norms, and customs [4]; and most importantly, the management of interpersonal communication boundaries [33].	Hypotheses 2 and 3
Dialectic/non-monotonic	In social interactions where privacy exerts its effects, two types of balances are maintained by each person: a balance between desired privacy and actual privacy [4], and a balance between need for privacy and need for disclosure [33,66]. That is, privacy is a dialectic process with a non-monotonic attribute [4,66], and an optimal (or satisfying) level of privacy is determined by the privacy calculus [33].	Hypotheses 4 and 5

3.1. Disposition to privacy and website-specific privacy concerns

As disposition to privacy represents a general attitude toward privacy while website-specific privacy concerns represent situation-specific attitudes, there is a potential relationship between the two. Attitude theory [1,2] suggests that a person's general attitude (or belief) about objects or events, once activated, would influence the evaluation of specific objects or events and therefore the situational attitudes. In terms of online privacy, it implies that disposition to privacy would influence the privacy attitude toward a particular website (i.e., website-specific privacy concerns). The above review (see Table 1) provides several reasons of their connection. First, disposition to privacy is the desired or expected control of personal information. This implies that when a person visits a website, he or she faces the risk of losing or shifting the control of personal information to the website, and the risk of losing the control leads to privacy concerns [69]. This is especially true when customers are required to provide personal information for needed products or service. Even though some websites may not explicitly collect customer information, they may implicitly collect information such as page views and clickstream and sell the information to third parties (for advertising purposes, for example), causing privacy concerns [60]. Second, disposition to privacy is the desire for an ideal balance between openness and closeness in inter-personal relationships, and the balance is regulated through the boundary control process [4]. However, it takes time and energy to delineate the inter-personal boundary and to balance it, and such balance is especially difficult to achieve due to the lack of information about the website (e.g., information asymmetry). The imbalance is even worse when the website conducts opportunistic behavior in dealing with customer information [51]. Third, the idiosyncratic attribute of disposition to privacy suggests that people differ in their extent of privacy expectations, as some are privacy fundamentals while others are privacy pragmatists or unconcerned [66]. Since privacy concerns are caused by the discrepancy between expected privacy and actual privacy, it implies that when people who have different initial expectations for privacy visit the same website, they may experience different discrepancies between their privacy expectations and actual privacy on the website, leading to varied privacy concerns. For example, many websites use cookies to track user information, which may cause different privacy concerns for those who accept or do not accept cookie use [48]. In sum, the desired control of privacy versus potential loss of control, the need for a balanced inter-personal relationship versus the potential imbalance caused by the uncertainties in interaction with a website, and the potential discrepancy between expected privacy and actual privacy all point to a positive impact of disposition to privacy on website-specific privacy concerns.

The online environment poses challenges to the protection of individual privacy, as technologies are available to collect customer information without their explicit consent [60,63]. Online firms that collect the information may also use it for secondary purposes and may handle the information unfairly [46]. Individuals who are aware of such privacy risks would express concerns about how their information is collected and used by a website [9,72]. This is especially true when the person has limited knowledge of the information practice on the website, so that disposition to privacy provides the "salient cue" [1] to assess privacy risks on the website, based on which the privacy attitude is developed and the necessary self-protection behavior is initiated [14]. Therefore, we hypothesize:

H1. A persons' disposition to privacy has a positive impact on the person's privacy concerns about a website.

3.2. Website reputation, familiarity, and website-specific privacy concerns

Perceptions about a specific object or event, such as the privacy concerns about a website, are subject to the influence of not only a person's general attitudes and beliefs but also contextual factors through

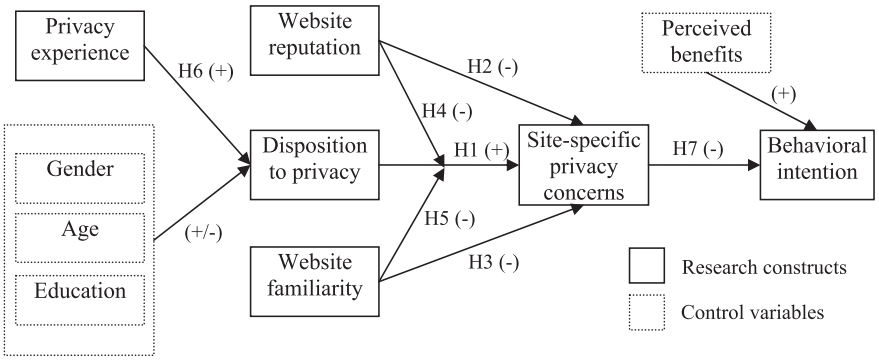

Fig. 1. Research model.

the mechanisms known as persuasion and social influence [67]. This study examines two contextual factors that may influence individuals' privacy perceptions: the reputation of a website and personal familiarity with the website. A firm's reputation is an overall assessment of the firm's product and service expertise, social characters, customer experience, and credible communications about the firm's abilities to serve customers [56]. It provides important cues of how the firm handles customer affairs, including their privacy [31]. Studies show that the reputation of a website has a direct impact on privacy concerns and also an indirect impact through the mediating role of trust on the website [5,18,30,31]. This is because information exchange is necessary for the fulfillment of online transactions [28], which involves both an economic contract (i.e., purchasing products or service) and a social contract (i.e., providing personal information). The opportunistic behavior of online firms in dealing with customer information, however, may violate the social contract and cause privacy concerns [51].

It should be noted that in recent years several big, reputable firms such as Apple Inc. and Facebook Inc. have been reported and criticized for their misconduct in handling customer information on their websites [27,69]. In fact, these firms were under close watch by the media for wrongdoings, and fortunately they responded promptly to the public outcry by adjusting their privacy policies, preventing or minimizing the reputation loss. On the other hand, disreputable websites, usually smaller ones, are seldom the targets of the media for such misconduct, but this alone doesn't mean that they are doing a better job than reputable firms in protecting privacy.

It should also be noted that reputation is built on many facets, and the respect for customer privacy is one of them. Nevertheless, a reputable firm would enjoy the "halo effect" [29] since the consumers may believe that if the firm is doing outstanding jobs in other aspects, it would do equally well in privacy protection. That is, the customers may believe that reputable websites can handle customer information with competence and commitment due to their common business practices, ethical standards, and even the pressure from the media, but disreputable websites may lack the competence or commitment to protect privacy. Given all these reasons, we hypothesize that:

H2. Perceived reputation of a website has a negative impact on a person's privacy concerns about the website.

Personal familiarity with a website, or website familiarity, refers to a consumer's degree of acquaintance with the website, including knowledge of the website and relevant procedures such as information search on the website [21]. It represents a social–relational factor that enables the customer to assess the overall experience in interacting with the website, and is a precondition of trust [24,31,64]. Familiarity with a website has a potential impact on consumer behavior: on a familiar website, the customer gets the knowledge about what information is collected by the website, how that information is used, and/or what to do to control the information and its use; such kind of knowledge is hard to get on an unfamiliar website. All these comply with the core requirements of the Fair Information Practice (e.g., informed consent, reserve, and exit) and deal directly with privacy concerns [46]. While the experience with a website may allow the customers to recognize potential privacy risks, it may also help them to devise best response strategies in reaction to the potential risks and subsequently lower the privacy concerns.

Studies also show that familiarity with a website results in a feeling of intimacy by the customer [36], and intimacy, which is a means to privacy [65,66], encourages the self-disclosure of personal information to the website and the continuous use of the website. In fact, the literature shows a positive relationship between familiarity and good feelings about a website such as liking (e.g., familiar brands appear to be better liked than unfamiliar brands) [36], suggesting a negative impact of familiarity on website-specific privacy concerns. Considering both the cognitive (i.e., knowledge about the information practice of the website) and affective (i.e., intimacy with the website) functions of familiarity, we expect, in accordance with the equifinal attribute of privacy in Table 1, that familiarity would have a negative impact on privacy concerns. We hypothesize:

H3. Personal familiarity with a website has a negative impact on a person's privacy concerns about the website.

3.3. Potential moderating effects among the antecedents

We expect perceived reputation and personal familiarity to have a moderating effect on the relationship between disposition to privacy and website-specific privacy concerns. As mentioned above, disposition to privacy represents a general attitude toward privacy while website-specific privacy concerns represent a situational attitude. Meanwhile, reputation and familiarity are both contextual beliefs, or "situational cues" [2], as they are beliefs about a particular website. According to attitude theory, the impact of an attitude or belief on a situational attitude or belief is contingent on its accessibility and salience, and in general, contextual beliefs are more accessible and salient than general beliefs in attitude formation [1]. Therefore, whenever the contextual beliefs or situational cues (e.g., perceived reputation and personal familiarity) are accessible, the salience of general attitudes and beliefs (e.g., disposition to privacy) would be attenuated. For example, if a person is not familiar with a website, then the personal belief about the website is not accessible, so that the general attitude and belief would become a salient cue to evaluate the website. On the other hand, if a person is familiar with a website, then the personal belief about the website would play a more salient role than the general attitude and belief.

Based on attitude theory, we examine how reputation and familiarity exert the moderating effects. As mentioned above, the impact of disposition to privacy on website-specific privacy concerns reflects the perceived discrepancy between a person's desired privacy and

actual privacy (as perceived by the person), so that the impact would be weaker if the discrepancy could be reduced by a third factor. A few studies on the moderating effect of familiarity have been reported in the literature [12,64] but to our best knowledge, none has been reported about the moderating effect of reputation. Therefore, we examine familiarity first.

A couple of studies tested the moderating effect of familiarity in the online environment. Casalo et al. [12] showed that familiarity with a website moderates the impact of contextual factors (such as website usability) on customer loyalty, as it enables the customer to evaluate contextual information differently: less familiarized customers use external information (such as word-of-mouth) whereas more familiarized customers prefer internal information (such as personal experience). In terms of online privacy, Van Slyke et al. [64] examined the moderating effects of familiarity on the impact of generalized privacy concerns on both trust beliefs and risk beliefs, suggesting that when customers become more familiar and experienced with a website, their generalized privacy concerns will be of less importance to trust and risk beliefs because the first-hand experience provides evidence that they can trust the website. Unfortunately, the moderating effects in Van Slyke et al.'s study were not supported.

While the relationships examined in the above two studies differ, they both indicate that familiarity provides situational cues, such as first-hand experience, to the consumer to evaluate a website. In terms of website-specific privacy concerns, we argue, following the logic, that familiarity with a website helps to alleviate some of the privacy concerns caused by disposition to privacy. First, familiarity helps to reduce the privacy risks due to its cognitive function. This doesn't mean that familiarity may totally eliminate the potential risks; instead, it means that the customer is better equipped with necessary knowledge or strategies to deal with the risks, which is known as the risk calculus [39]. Second, familiarity helps to build and maintain a balanced and intimate relationship between the person and the website, which alleviates the potential risks perceived by the person and thus reduces the privacy concerns. In both scenarios, the salience of personal privacy disposition is weakened. On an unfamiliar website, then, neither of the benefits of familiarity may exist, so that disposition to privacy becomes the primary information cue. Taken these together, we suggest that familiarity would have a negative impact on the relationship between disposition to privacy and website-specific privacy concerns.

For the moderating effect of reputation, we suggest, similar to website familiarity, that it would negatively influence the relationship between disposition to privacy and website-specific privacy concerns. On a more reputable website, although consumers may have concerns about information privacy because of their privacy disposition, such concerns could be alleviated because of the reputation of the website. On a less reputable website, the privacy concern would be even stronger because of the uncertainties associated with privacy risks. If the reputation of a website is unknown or neutral, disposition to privacy would then have its pure effect on privacy concerns since it is the only information cue.

We emphasize that although reputation and familiarity may both moderate disposition to privacy, there is a distinction between the two: reputation focuses on external information cues that come from other parties such as other customers' experiences or word-of-mouth, while familiarity focuses on internal information cues that are derived from the personal experience with the website. These two sources of information are complementary, so that their moderating effects both exist. It is therefore hypothesized:

H4. For a more reputable website, the relationship between a person's disposition to privacy and website-specific privacy concerns is weaker, as compared to a less reputable website.

H5. For a more familiar website, the relationship between a person's disposition to privacy and website-specific privacy concerns is weaker, as compared to a less familiar website.

3.4. Antecedent of privacy disposition

Due to the limited empirical studies on the antecedents of disposition to privacy, we explore factors that may explain its development. A promising factor is the privacy experience of a person: studies show that prior experience with privacy risks has a strong impact on the enduring privacy beliefs of a person [9,61]. In other words, the accumulation of experience with privacy risks enhances the awareness of those risks and therefore enhances the overall privacy concerns and need for privacy. This conforms to Laufer and Wolfe's [33] theory that relates the development of privacy disposition to one's life cycle, which also refers to the developmental attribute of disposition to privacy in Table 1. We hypothesize:

H6. A person's experience with privacy risks has a positive impact on the person's disposition to privacy.

3.5. Behavioral consequence of privacy concerns

We expect a direct impact of website-specific privacy concerns on a person's behavioral intention to use the website for information inquiry. As this relationship has been well studied in privacy literature [38,61], the rationale is not belabored. Although we observe in the literature review that disposition to privacy is also "instrumental," as it determines the information disclosure behavior of a person (see Table 1), we argue that its impact in a specific context is fully mediated by the context-specific privacy concerns (i.e., what the actual privacy may seem to be). Therefore, we hypothesize:

H7. A person's privacy concerns about a website have a negative impact on the person's behavioral intention to use that website.

3.6. Control variables

We include two sets of control variables in this study, one regarding the behavioral intention and the other regarding disposition to privacy. Studies on privacy calculus [61] suggest that a person's behavioral intention to disclose information to a website is jointly influenced by privacy concerns and expected benefits (i.e., desire for disclosure) [31]. The expected benefits include both monetary rewards and non-monetary rewards. As this study examines a person's general intention to use a website, perceived usefulness of a website [71] is deemed an appropriate surrogate. We expect perceived benefit (i.e., usefulness) of a website to have a positive impact on a person's behavioral intention to use the website.

As for disposition to privacy, trait theories suggest that demographic factors may have a potential impact on a person's privacy beliefs [61], and the developmental theory of privacy also suggests that individual factors play important roles in privacy formation [33]. Some of the demographic factors have been empirically tested in literature, of which the gender, age, and education are widely discussed [38]. In general, gender has a relatively consistent impact on privacy beliefs, as women are more concerned about privacy than men; the impacts of age and education are, however, inconsistent across studies [38]. Most studies on demographic factors focused on Internet or website privacy concerns, but few have tested their impact on disposition to privacy. Therefore, we include the three demographic factors as control variables to test their impact on disposition to privacy.

4. Research method

4.1. Research design

We conducted a survey to empirically test the research model by measuring individuals' self-reported privacy perceptions about websites and their assessment of other antecedent and consequence factors. Following the practice of other scholars [8,51,69], we chose multiple

websites with varied reputations in the study, including two online travel agencies (*Expedia.com* and *Travels-web.com*), two online financial service providers (*Scottrade.com* and *Nobletrading.com*), and two online auction sites (*Ebay.com* and *Bigdeal.com*). For each category of websites, we selected one that is of relatively higher reputation (including *Expedia*, *Scottrade* and *Ebay*) and one that is of relatively lower reputation (including *Travels-web*, *Nobletrading* and *Bigdeal*). The selection process was as follows. First, three categories of e-commerce websites were randomly chosen, and for each category, a number of candidate websites were recognized through the search engine. Their TV commercials were then searched for online, based on which the comments by users were examined to gauge their reputations. The financial information (such as revenues) of the websites was also recognized from online sources to compare their market positions, which also indicates their reputations. Combining all the information, we chose two websites in each category that we believe have distinct reputations. As the judgment of reputations was subjective in this process, we conducted further tests on the survey data to verify our selection.

4.2. Measurement items

All the items that measure the latent constructs were adopted from existing literature. These items, listed in the Appendix A, show proper psychometric properties in their original literature. Each manifest variable was measured with a seven-point Likert scale ranging from 1 (referring to low reputation, unfamiliar, or unconcerned, etc.) to 7 (referring to high reputation, very familiar, or very concerned, etc.). To reduce common method bias in the self-reported survey, we reversely worded several items to reduce the social desirability bias [54], and used statistical methods later to verify the existence of the common method bias, explained in Section 5.1. Each of the demographic factors, including gender, age, and education, was measured by a single item.

4.3. Data collection process

The survey proceeded as follows. First, the participants completed the portion of the survey that measures their disposition to privacy and privacy experience. Then, each participant was asked to visit a website listed on the survey questionnaire, which is randomly assigned. After that, the participant filled in the rest of the survey to capture their assessment of the reputation of the website, personal familiarity with the website, privacy concerns, and behavioral intentions. Finally, demographic information was collected from the participants.

The survey was conducted between April and November of 2011. The participants included faculty and staff from a private college, business people from a local business association, residents from a local community, and graduate students majoring in business from a mid-western university. All participants were from the United States. The employment of multiple types of respondents in the study helps to combat issues with student-dominated samples in privacy research [10,38,50]. A total of 264 questionnaires were sent to the faculty and staff via campus mails, with an additional 30 questionnaires handed to the business peoples and residents directly and 40 questionnaires handed to the graduate students in class. Two rounds of email reminders were sent to the faculty and staff, but no formal reminder was given to the other subjects. A total of 110 responses were received, yielding a 32.9% response rate. Descriptive information of the responses is listed in Table 2.

A possible reason of the relatively low response rate, especially among the faculty and staff, is the fact that each participant was required to visit a website to finish the survey. To test the potential non-response bias, we compared early respondents (before the first email reminder) and late respondents (after the first email reminder) based on their genders ($F = .19$, $p = .67$), age groups ($F = 2.81$, $p = .10$), education ($F = 1.36$, $p = .25$), years of Internet use ($F = .64$, $p = .42$), daily Internet use ($F = 1.63$, $p = .21$), and the websites (i.e., high reputation websites versus low reputation websites; $F = .60$, $p = .44$). None of these factors show significant differences, suggesting the lack of non-response bias in the data.

5. Data analysis and results

We use the Partial Least Squares (PLS) method to test the research model due to the exploratory, instead of theory-testing, purpose of the study [16], and use the SmartPLS software package [57] to analyze the data. SmartPLS assesses the psychometric properties of the variables directly and performs the bootstrapping process to test the significance of path coefficients. We first test the psychometric properties of the measurement items and then the research model. Post-hoc analyses are also conducted.

5.1. Test of measurement items

Table 3 reports the Internal Consistency Reliability (using Cronbach's alpha), Composite Reliability (CR) and the Average Variances Extracted (AVE) of each latent construct. The correlations between the constructs are also reported in the table along with the square roots of the AVE on the diagonal of the correlation matrix. All the reliability measures are above the threshold level of .7 [20], indicating acceptable reliabilities. The square root of the AVE of each construct is greater than its correlations with other constructs. The AVE of the website-specific privacy concerns construct is slightly lower than the minimum level of .5 [20]. This may be caused by the use of reversed wording (two out of six items) in the survey; nevertheless, the factor loadings of its manifest items (see the Appendix A) are all above .5, suggesting that the constructs exhibit acceptable convergent validity. The discriminant validity is examined by the factor loadings and cross-loadings. All factor loadings exceed the minimum level of .5 with no significant cross-loadings detected, suggesting sufficient discriminant validity.

As the common method bias may still persist in the data despite the use of reverse-worded items in the questionnaire, we used a couple of methods to test it, including Harman's single-factor test and the common method factor test [54]. For the single-factor test, an unrotated exploratory factor analysis (using SAS proc factor) on all manifest variables of the latent constructs yielded a six-factor structure with the first factor explaining 47.7% of variances in the data, lower than the suggested 50% cutoff level [54]. For the common method factor test, we followed the approach illustrated in Facteau et al. [19] to conduct a series of confirmatory factor analysis (using SAS proc calis) to compare the model fit of four competing models: the null model with manifest variables only ($\chi^2(378) = 2835.2$, GFI = .43), the method model with the common method factor ($\chi^2(349) = 1659.9$, GFI = .43), the measurement model with latent constructs ($\chi^2(329) = 504.2$, GFI = .76), and the measurement plus method factor model with both latent constructs and the common method factor ($\chi^2(293) = 410.8$, GFI = .79). The results show that the addition of the common method factor, as expected [19], improves the overall model fit in terms of chi-squares differences. Nevertheless, its contribution to the total variances in the data, 25.9% (calculated based on the sum of squares of the method factor loadings), is not comparable to the variances explained by the theoretical constructs (40.9%; calculated based on the sum of squares of the latent factor loadings). Therefore, the data do not suffer from the common method bias.

5.2. Test of the research model

The research model is estimated via the bootstrapping process in SmartPLS using 200 samples. The results are reported in Fig. 2; factor loadings of the manifest variables of the latent constructs are reported in the Appendix A. All the loadings are above .5. The results confirm our expectation that disposition to privacy, website reputation, and

Table 2
Descriptive information of the survey responses.

Demographic factors	Frequency	Demographic factors	Frequency
Gender		Years of Internet use	
Female	72	Less than 1 year	1
Male	37	1–3 years	0
Age		4–6 years	13
25 or under	18	7 years or more	95
26–35	32	Daily Internet use	
36–45	18	Less than 1 h	5
46–55	21	1–2 h	31
56 or older	19	3–4 h	33
Education		5–6 h	27
College degree or below	52	7 h or more	12
Master's degree	35		
Doctoral degree	35		

website familiarity each have a significant impact on website-specific privacy concerns, supporting H1 ($\beta = .202$, $p < .05$), H2 ($\beta = -.275$, $p < .01$), and H3 ($\beta = -.202$, $p < .01$). Neither of the moderating effects reached significance at .05 level, rejecting H4 ($\beta = -.067$, $p > .1$) and H5 ($\beta = -.191$, $p > .1$); nevertheless, both are in the expected direction. The model explains 31% of the variance in website-specific privacy concerns.

The four antecedents to disposition to privacy explain 8% of the variance in this construct. Nevertheless, only privacy experience is significant, supporting H6 ($\beta = .192$, $p < .05$), and none of the control variables (i.e., gender, age, and education) is significant. Finally, the impact of website-specific privacy concerns on behavioral intention is significant at .01 level, supporting H7 ($\beta = -.413$, $p < .01$). The impact of perceived benefits on behavioral intention is also confirmed ($\beta = .593$, $p < .01$). These two variables together explain 70% of the variance in behavioral intention, supporting the privacy calculus.

5.3. Post-hoc analyses

As mentioned above, a potential threat to the validity of the study is the selection of the six websites, since we are uncertain whether the reputations of the websites, as perceived by the subjects in the survey, are consistent with our selection. To verify the perceived reputations of the websites, we conducted t-tests to compare the reputation measures of each pair of websites. The results are shown in Table 4. Consistent with our selection, the two travel service websites have different reputations (significant on three out of four items), and so do the two online auction websites (significant on all four items). For the financial service websites, the differences are insignificant but in the expected direction. Overall, our selection of the websites, in terms of their distinct reputations, is valid. This allows us to conduct further analyses.

Table 3
Psychometric properties and correlations of the constructs.

Constructs	ICR	CR	AVE	1.	2.	3.	4.	5.	6.	7.
1. Disposition to privacy	.84	.91	.76	**.87**						
2. Perceived reputation	.91	.94	.79	−.03	**.89**					
3. Personal familiarity	.93	.95	.82	−.02	.45	**.91**				
4. Privacy concerns	.74	.82	.43	.24	−.43	−.35	**.66**			
5. Privacy experience	.91	.94	.84	.20	.03	.11	.20	**.92**		
6. Perceived benefits	.97	.98	.91	−.11	.57	.50	−.40	−.05	**.95**	
7. Intention	.92	.94	.80	−.21	.62	.52	−.63	−.08	.75	**.89**

Note: ICR — Internal consistency reliability (Cronbach's α); CR — Composite reliability; AVE — Average variance extracted. Values on the diagonal of the matrix are the square roots of the AVE of each construct.

We measured website reputation as an individual level factor based on personal perceptions, a typical approach in survey studies [13]. The results could be different if we had treated reputation as an organizational level factor invariant at the individual level, a typical treatment in experimental research [5,18]. To examine the potential impact of the different treatments of the reputation variable, we coded the reputations of the websites with 1 indicating high reputation and 0 indicating low reputation, and retested the model. The results confirmed our concern: the path coefficient between website reputation and privacy concerns is −.18 ($t = 1.37$), which, although in the right direct, does not reach significance. We question whether different mechanisms are in place to determine the privacy concerns about websites with different reputations (e.g., high reputation versus low reputation), and we conduct the following two tests to address this issue.

First, we retested the research model for high reputation websites; those non-significant relationships (see Fig. 2) were excluded from the test. The results are shown in Fig. 3, which are consistent with the results in Fig. 2 (with both high and low reputation websites). Second, we retested the research model for low reputation websites; similarly, non-significant relationships from prior tests were excluded. The result shows the distinction: the impact of perceived website reputation on privacy concerns is still significant ($\beta = -.404$, $t = 4.09$), but the impact of website familiarity is insignificant ($\beta = .391$, $t = 1.46$). A potential reason for the diminishing effect of familiarity, as other studies imply [21], is that website reputation, which is a primary basis of trust, may mediate the impact of personal familiarity. We therefore included a direct path from familiarity to reputation and reran the model. The result is shown in Fig. 4, suggesting that perceived website reputation is a full mediator of website familiarity for low reputation sites. In sum, the main relationships hypothesized in our research model in Fig. 1 are supported across the websites, although distinctions regarding the impact of familiarity may be noticed between websites with varied reputations.

It should be noted that website familiarity has been commonly operationalized as a continuous variable measuring personal perceptions [24,31,36]. Therefore, we deem it inappropriate to dichotomize the variable and test its impact on privacy concerns as we did for website reputation. It should also be noted that we included gender, age, and education as control variables for disposition to privacy while past research also controlled these variables for site-specific privacy concerns and even behavioral intention [38]. Therefore, we conducted post-hoc analyses on their impacts on both constructs. The results show that age has a positive impact on site-specific privacy concern ($\beta = .162$, $t = 1.95$, $p = .05$) and a negative impact on behavior intention ($\beta = -.151$, $t = 2.67$, $p < .01$). None of the other control variables are significant, and the results regarding the hypotheses are unchanged.

6. Discussion and concluding remarks

6.1. Contributions of the study

The study has several potential contributions. First, the systematic review on disposition to privacy and the recognition of its key attributes in Table 1 fill the gap in the e-commerce literature. The test on its direct impact on website-specific privacy concerns highlights its importance to online privacy, calling for more attentions to this critical concept in further research. For example, a person's social environment plays critical roles in the development of privacy disposition, suggesting the need to study how the online environment may shape a person's privacy perception, especially for young generations. Second, the study extends the literature on the relationship between disposition to privacy and privacy concerns [55,70], especially Xu et al.'s [69] study on website privacy concerns. We notice three major differences between Xu et al.'s study and ours. For one, the contextual factors are different. As mentioned in Section 1, Xu et al. studied privacy policy and industry self-regulation despite the declining readability of privacy policies [47] and few people ever noticing or reading the policies [45,49]. Since the reputation of a website and

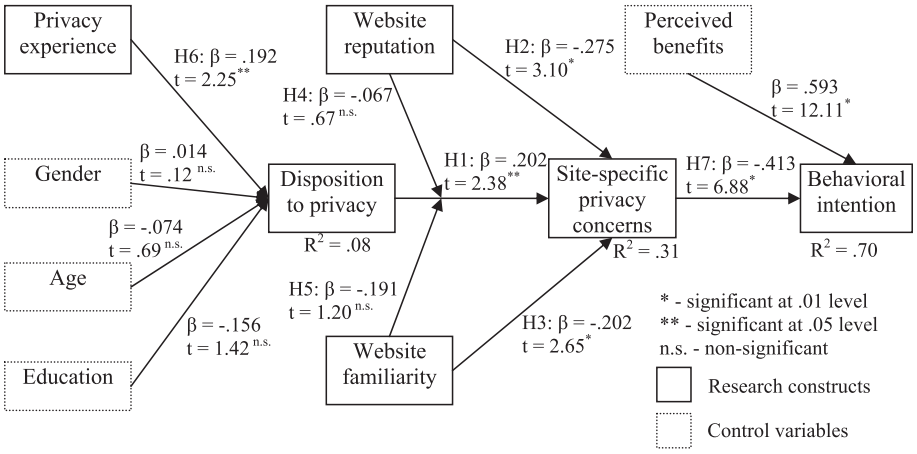

Fig. 2. Significance test of the full research model.

personal familiarity with a website are both closely related to online privacy [5,18,64], the inclusion of both factors may help to address the issue. Two, Xu et al. did not test the direct impact of contextual factors on website-specific privacy concerns, and nor did they test the potential interactions between contextual factors and disposition to privacy. Our study therefore provides additional insights into these factors. Although the interactions were not significant in this study, we discuss potential reasons later. Three, Xu et al. employed only student subjects in their experiment, which may suffer from the generalizability issue. Our study employed a combination of student and non-student subjects to help address the issue. Therefore, we deem our study an importance supplement to existing literature. Finally, our study contributes to the literature via the investigation of the antecedents to disposition to privacy, which has been seldom explored in the e-commerce literature. Due to the limited number of antecedents tested, we expect future research to study additional factors that may account for this critical concept.

Two major hypotheses in the study, the moderating effects of reputation and familiarity, were not supported; this deserves further attention. To gain insight into the impact of both factors, we split the sample into two groups based on website reputations (i.e., high reputation versus low reputation) and then personal familiarity (i.e., high familiarity versus low familiarity), and conducted ordinary regression analysis on the impact of disposition to privacy on website-specific privacy concerns in each group. The factor scores of the latent constructs were used for analysis, and the results are reported in Table 5. It shows that the impact of disposition to privacy on website-specific privacy concerns is significant in both low reputation ($\beta = .16$; $p = .06$) and low familiarity ($\beta = .14$; $p = .06$) groups, but insignificant in both high reputation ($\beta = .12$; $p = .13$) and high familiarity ($\beta = .13$; $p = .20$) groups. Consistent with the above analysis, it suggests that for low reputation or less familiar websites, disposition to privacy plays important roles in forming privacy concerns. On the other hand, for high reputation or more familiar websites, the role of disposition to privacy in forming privacy concerns diminishes. Nevertheless, as the difference between the regression coefficients is small in each pair of groups, possibly due to small sample sizes, the hypothesized moderating effects did not reach significance in the whole sample. It is therefore recommended that future research be conducted to collect more data to retest the model.

6.2. Implications of the study

This study has implications for research and practice. From the behavioral decision-making point of view, it is important to recognize the information cues that consumers use to develop situational privacy beliefs and intention. The study confirms three sources of information for website-specific privacy concerns, suggesting that both personal values (i.e., disposition to privacy) and contextual factors (i.e., reputation and familiarity) should be included in future research on individual privacy concerns and behavior. In addition, the study shows that the significance of each factor may be influenced by the magnitude of the other factors. For example, Fig. 4 illustrates that when the reputation of a website is low, the impact of familiarity on website-specific privacy concerns is attenuated and fully mediated by reputation. Also, Table 5 shows that in the scenarios of low reputation and low familiarity, disposition to privacy is a significant predictor of website-specific privacy concerns; in the scenarios of high reputation and high familiarity, however, the impact of disposition to privacy becomes less important. While it's too early to draw the final conclusion, the results seem to comply with the assertion that the influence of values and beliefs on individual behavior is contingent on the accessibility and salience of those values and beliefs [1,2]. Compared to the other two factors, website reputation seems to be a more salient predictor of website-specific privacy concerns. Therefore for online firms, the reputation building that emphasizes privacy protection should be given a higher priority in addressing privacy concerns.

The study confirms that disposition to privacy is an important predictor of a person's website-specific privacy concerns. This implies that online firms should make efforts to understand their customers' privacy dispositions and design products and service based on their privacy preference. For example, Lee et al. [35] suggest that online firms should offer standard products and service (which requires less or no personal information) to privacy fundamentalists, and personalized products and service (which requires more personal information)

Table 4
Comparison of reputations between each pair of websites.

Measurement items	Travel service		Financial service		Online auction	
	Expedia	*Travels-web*	*Scottrade*	*Nobletrading*	*Ebay*	*Bigdeal*
Item 1	5.44 (.70)[a*]	4.11 (1.33)	5.37 (1.21)[n.s.]	4.75 (1.07)	5.60 (.91)[*]	3.83 (1.11)
Item 2	5.06 (.94)[*]	3.79 (1.47)	4.58 (.96)[n.s.]	4.65 (.99)	5.47 (1.13)[*]	3.92 (.29)
Item 3	5.28 (.83)[*]	4.11 (1.20)	5.05 (.97)[n.s.]	4.75 (1.12)	5.73 (.70)[*]	4.08 (1.16)
Item 4	4.78 (1.00)[n.s.]	4.21 (1.08)	4.95 (1.18)[n.s.]	4.60 (1.19)	5.60 (.91)[*]	3.92 (.51)

Note: a — mean value and standard deviation (in parentheses); * — significant at .01 level; n.s. — non-significant.

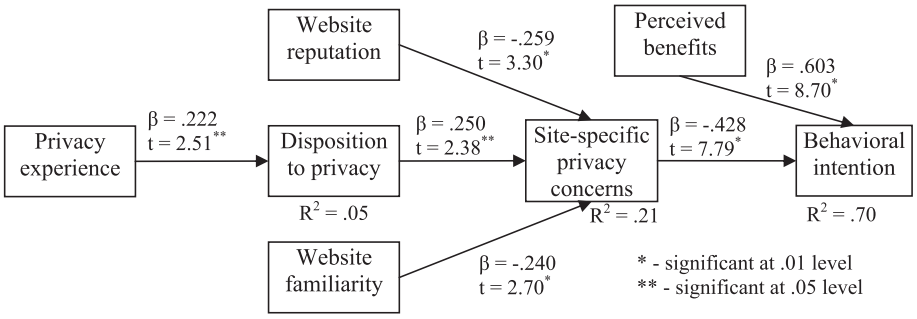

Fig. 3. Retest of the research model for high reputation websites.

to privacy unconcerned; for privacy pragmatists, they may offer both. Further research is needed to help online firms to better understand their customers' privacy dispositions.

Finally, familiarity has an impact on privacy concerns, suggesting that social relationships should be sought after to address some of the privacy issues. Social response theory suggests that a reciprocal relationship can be established between a customer and a website that encourages the self-disclosure of information by the customer [71]. This reciprocal relationship is necessarily built on personal familiarity with a website. Nevertheless, as the impact of familiarity can also be mediated by website reputation (as Fig. 4 shows), it suggests that familiarity should not be substituted for reputation.

6.3. Limitations of the study

This study contains a number of limitations that may be addressed in future research. First, we adopt the privacy-as-control perspective in the study, despite the fact that other perspectives also exist in literature [61]. The other perspectives provide additional insights to the privacy concept, which should be incorporated in further research. For example, privacy-as-commodity is a typical approach to studying privacy from an economic point of view [59], which may help online firms to develop incentive schemes to elicit customer information.

Second, other privacy beliefs such as general concerns for online privacy [38] may also influence website-specific privacy concerns. A few studies examined the distinctions between the two constructs, although empirical evidence has yet been found regarding their connections [37,38,40]. Nevertheless, future research should be conducted to examine how privacy beliefs, such as general concerns for privacy, may influence the formation of website-specific privacy concerns.

Third, the study suffers from the limited number of contextual factors. As we mentioned above, other contextual factors such as privacy policies [69], website informativeness [51], and types of information [42] all have potential impacts on privacy concerns. For example, Malhotra et al. [42] show that the type of information requested influences both trusting belief and risk belief on a website, although its impact on privacy concern is not tested. Further research shows an interactive effect of information type and personal familiarity (in terms of frequency of contact with a website) on privacy concerns [58]. These multiple contextual factors could be further investigated along with disposition to privacy.

Fourth, the selection of the websites may suffer from the misjudgment of the authors, as the selection was based on the authors' subjective assessment of their reputations. In fact, several online sources provide customer ratings of e-commerce websites (such as *toptenreviews.com*), which may serve as a basis for selecting the research websites. Although the results in general support our research design (see Table 4), future research could be conducted to verify the model based on more scientific selection of websites using third-party ratings.

Fifth, each of the subjects was asked to complete the survey on only one website, which was not helpful in testing the stability of their disposition to privacy across contexts. It would be better to conduct repeated measures on dispositions to privacy and website-specific privacy concerns at different times and for different websites to test not only the stability of disposition to privacy but also the robustness of its impact on website-specific privacy concerns across websites.

Finally, only one significant antecedent to disposition to privacy was recognized, suggesting that additional efforts are needed to recognize other sources of privacy disposition. For example, education was not found to have a significant impact on privacy disposition, partly because we measured general education (e.g., a college degree). Other more specific education related to Internet and privacy issues may show a significant impact, although additional evidences are needed [32]. All these issues should be addressed to further knowledge on online privacy.

In sum, this study confirms the impact of disposition to privacy, website reputation, and personal familiarity on website-specific privacy concerns. It highlights the influence of both individual values and contextual factors on the development of situational privacy beliefs, calling for more attention to individual disposition to privacy. The key attributes of disposition to privacy, as summarized in Table 1, may serve as the basis for further research on this critical construct in the e-commerce literature.

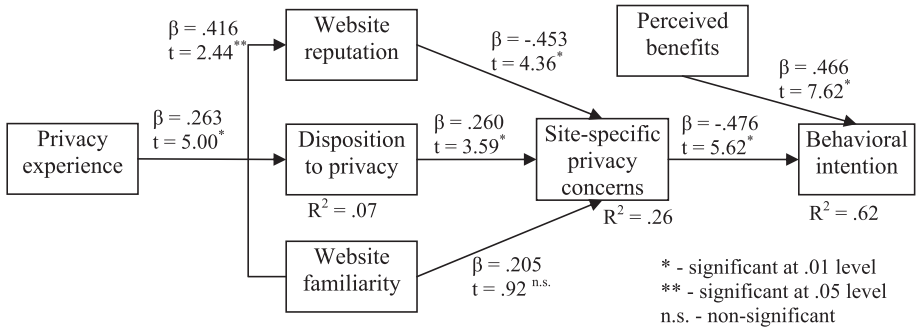

Fig. 4. Retest of the research model for low reputation websites.

Table 5
Regression of website-specific privacy concerns on disposition to privacy by groups.

	High reputation			Low reputation			High familiarity			Low familiarity		
	β	t	p	β	t	p	β	t	p	β	t	p
Intercept	3.48	8.12	<.001	3.88	8.74	<.001	3.30	6.41	<.001	3.88	9.76	<.001
Disposition to privacy	.12	1.53	.13	.16	1.96	.06	.13	1.29	.20	.14	1.91	.06
R^2 (Adjusted R^2)	.04 (.03)			.07 (.05)			.04 (.02)			.05 (.04)		

Appendix A. Measurement items of latent constructs

Measurement item	M	S.D.	L
Disposition to privacy [69]			
Compared to others, I am more sensitive about the way other people or organizations handle my personal information.	5.06	1.47	.91
Compared to others, I see more importance in keeping personal information private.	5.49	1.53	.92
Compared to others, I am less concerned about potential threats to my personal privacy. (reverse-worded)	5.07*	1.76	.78
Website reputation [13]			
This website has a good reputation.	4.93	1.23	.92
This website has a good reputation compared to other rival websites.	4.61	1.16	.86
This website has a reputation for offering good products or services.	4.88	1.15	.92
This website has a reputation for being respectful to its customers.	4.70	1.15	.85
Website familiarity [21]			
I am familiar with this website.	3.34	2.18	.89
I am familiar with conducting transactions (such as buying products or services) on this website.	3.09	2.26	.90
I am familiar with searching for information on this website.	3.52	2.22	.92
I am familiar with inquiring about information on this website.	3.38	2.17	.91
Website-specific privacy concerns [51]			
I am concerned that this website is collecting too much information about me.	3.80	1.36	.59
It does not bother me when this website asks me for personal information. (reverse-worded)	4.86*	1.52	.73
I am concerned about my privacy when browsing this website.	3.87	1.58	.60
I have no doubts about how well my privacy is protected on this website. (reverse-worded)	4.65*	1.40	.70
My personal information could be misused when transacting with this website.	4.51	1.20	.63
My personal information could be accessed by unknown parties when transacting with this website.	4.32	1.16	.67
Perceived benefit [22,71]			
The website improves my performance in searching for information I need.	4.24	1.32	.92
The website enables me to search for information faster.	4.48	1.20	.97
The website enhances my effectiveness in information search.	4.48	1.33	.97
The website increases my productivity in information search.	4.44	1.29	.96
Privacy experience [9]			
I have had bad experiences with regard to my online privacy before.	3.37	1.82	.94
I was a victim of online privacy invasion.	2.79	1.94	.94
I believe that my online privacy was invaded in by other people or organizations.	3.33	1.95	.87
Behavioral intention [9,23]			
I am willing to use this website in the future to inquire information I need.	4.34	1.73	.91
It is probable for me to disclose my personal information to this web for its products or services.	3.82	1.63	.88
I am willing to use this website in the future to compare products or services before I make a purchase from this or other websites.	4.44	1.65	.90
Given the need, I am willing to provide my personal information to this website in order to find specific products or services that fit me.	4.20	1.71	.88

Note: M — mean; S.D. — standard deviation; L — factor loading.
* The reverse-worded items were transformed based on the 7-point Likert scale.

References

[1] I. Ajzen, Nature and operation of attitudes, Annual Review of Psychology 52 (1) (2001) 27–58.
[2] I. Ajzen, M. Fishbein, The influence of attitudes on behavior, in: D. Albarracín, B.T. Johnson, M.P. Zanna (Eds.), The Handbook of Attitudes, Erlbaum, Mahwah, NJ, 2005, pp. 173–221.
[3] I. Altman, The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding, Brooks/Cole Publishing, Monterey, CA, 1975.
[4] I. Altman, Privacy: a conceptual analysis, Environment and Behavior 8 (1) (1976) 7–29.
[5] E.B. Andrade, V. Kaltcheva, B. Weitz, Self-disclosure on the web: the impact of privacy policy, reward, and company reputation, Advances in Consumer Research 29 (1) (2002) 350–353.
[6] C.M. Angst, R. Agarwal, Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion, MIS Quarterly 33 (2) (2009) 339–370.
[7] N.F. Awad, M.S. Krishnan, The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization, MIS Quarterly 30 (1) (2006) 13–28.
[8] G. Bansal, F.M. Zahedi, D. Gefen, The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: a multiple-context investigation, Proceedings of the Twenty Ninth International Conference on Information Systems, 2008.
[9] G. Bansal, F.M. Zahedi, D. Gefen, The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online, Decision Support Systems 49 (2) (2010) 138–150.
[10] F. Belanger, R.E. Crossler, Privacy in the digital age: a review of information privacy research in information systems, MIS Quarterly 35 (4) (2011) 1017–1041.
[11] S. Bellman, E. Johnson, S. Kobrin, G. Lohse, International differences in information privacy concerns: a global survey of consumers, Information Society 20 (5) (2004) 313–324.
[12] L. Casaló, C. Flavián, M. Guinalíu, The role of perceived usability, reputation, satisfaction and consumer familiarity on the website loyalty formation process, Computers in Human Behavior 24 (2) (2008) 325–345.

[13] L.V. Casalo, C. Flavian, G. Miguel, The role of security, privacy, usability and reputation in the development of online banking, Online Information Review 31 (5) (2007) 583–603.
[14] S. Chai, S. Bagchi-Sen, C. Morrell, H.R. Rao, S.J. Upadhyaya, Internet and online information privacy: an exploratory study of preteens and early teens, IEEE Transactions on Professional Communication 52 (2) (2009) 167–182.
[15] J. Chen, W. Ping, Y. Xu, B.C.Y. Tan, Am I afraid of my peers? Understanding the antecedents of information privacy concerns in the online social context, Proceedings of the Thirtieth International Conference on Information Systems, 2009.
[16] W.W. Chin, Issues and opinion on structural equation modeling, MIS Quarterly 22 (1) (1998) 7–16.
[17] M.J. Culnan, P.K. Armstrong, Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation, Organization Science 10 (1) (1999) 104–115.
[18] M.A. Eastlick, S.L. Lotz, P. Warrington, Understanding online B-to-C relationships: an integrated model of privacy concerns, trust, and commitment, Journal of Business Research 59 (8) (2006) 877–886.
[19] J.D. Facteau, G.H. Dobbins, J.E.A. Russell, R.T. Ladd, J.D. Kudisch, The influence of general perceptions of the training environment on pretraining motivation and perceived training transfer, Journal of Management 21 (1) (1995) 1–25.
[20] C. Fornell, D. Larcker, Evaluating structural equation models with unobservable variables and measurement error, Journal of Marketing Research 18 (1981) 39–50.
[21] D. Gefen, E-commerce: the role of familiarity and trust, Omega 28 (2000) 725–737.
[22] D. Gefen, E. Karahanna, D. Straub, Trust and TAM in online shopping: an integrated model, MIS Quarterly 27 (1) (2003) 51–90.
[23] D. Gefen, D. Straub, The relative importance of perceived ease of use in IS adoption: a study of e-commerce adoption, Journal of the Association for Information Systems 1 (8) (2000) 1–28.
[24] D. Gefen, D.W. Straub, Consumer trust in B2C e-Commerce and the importance of social presence: experiments in e-Products and e-Services, Omega 32 (6) (2004) 407–424.
[25] A. Haans, F.G. Kaiser, Y.A.W. de Kort, Privacy needs in office environments: development of two behavior-based scales, European Psychologist 12 (2) (2007) 93–102.
[26] I. Hann, K. Hui, S.T. Lee, I.P.L. Png, Overcoming online information privacy concerns: an information-processing theory approach, Journal of Management Information Systems 24 (2) (2007) 13–42.
[27] C.M. Hoadley, H. Xu, J.J. Lee, M.B. Rosson, Privacy as information access and illusory control: the case of the Facebook News Feed privacy outcry, Electronic Commerce Research and Applications 9 (1) (2010) 50–60.
[28] D.L. Hoffman, T.P. Novak, M.A. Peralta, Information privacy in the marketspace: implications for the commercial uses of anonymity on the Web, Information Society 15 (2) (1999) 129–139.
[29] B. Jin, J.Y. Park, J. Kim, Joint influence of online store attributes and offline operations on performance of multichannel retailers, Behaviour & Information Technology 29 (1) (2010) 85–96.
[30] A. Jøsang, R. Ismail, C. Boyd, A survey of trust and reputation systems for online service provision, Decision Support Systems 43 (2) (2007) 618–644.
[31] D.J. Kim, D.L. Ferrin, H.R. Rao, A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents, Decision Support Systems 44 (2) (2008) 544–564.
[32] D.J. Kim, C. Steinfield, Y.J. Lai, Revisiting the role of web assurance seals in business-to-consumer electronic commerce, Decision Support Systems 44 (4) (2008) 1000–1015.
[33] R.S. Laufer, M. Wolfe, Privacy as a concept and a social issue: a multidimensional development theory, Journal of Social Issues 33 (3) (1977) 23–42.
[34] C.H. Lee, D.A. Cranage, Personalisation-privacy paradox: the effects of personalisation and privacy assurance on customer responses to travel Web sites, Tourism Management 32 (5) (2011) 987–994.
[35] D.J. Lee, J.H. Ahn, Y. Bang, Managing consumer privacy concerns in personalization: a strategic analysis of privacy protection, MIS Quarterly 35 (2) (2011) 423–444.
[36] Y. Lee, O. Kwon, Intimacy, familiarity and continuance intention: an extended expectation–confirmation model in web-based services, Electronic Commerce Research and Applications 10 (3) (2011) 342–357.
[37] H. Li, R. Sarathy, H. Xu, Understanding situational online information disclosure as a privacy calculus, Journal of Computer Information Systems (2010) 62–71.
[38] Y. Li, Empirical studies on online information privacy concerns: literature review and an integrative framework, Communications of the Association for Information Systems 28 (28) (2011) 453–496.
[39] Y. Li, Theories in online information privacy research: a critical review and an integrated framework, Decision Support Systems 54 (1) (2012) 471–481.
[40] C. Liao, C.-C. Liu, K. Chen, Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: an integrated model, Electronic Commerce Research and Applications 10 (6) (2011) 702–715.
[41] M. Lwin, J. Wirtz, J.D. Williams, Consumer online privacy concerns and responses: a power-responsibility equilibrium perspective, Journal of the Academy of Marketing Science 35 (4) (2007) 572–585.
[42] N.K. Malhotra, S.S. Kim, J. Agarwal, Internet Users' Information Privacy Concerns (IUIPC): the construct, the scale, and a causal model, Information Systems Research 15 (4) (2004) 336–355.
[43] S.T. Margulis, On the status and contribution of Westin's and Altman's theories of privacy, Journal of Social Issues 59 (2) (2003) 411–429.
[44] S.T. Margulis, Privacy as a social issue and behavioral concept, Journal of Social Issues 59 (2) (2003) 243–261.
[45] D.B. Meinert, D.K. Peterson, J.R. Criswell, M.D. Crossland, Privacy policy statements and consumer willingness to provide personal information, Journal of Electronic Commerce in Organizations 4 (1) (2006) 1–17.
[46] S.J. Milberg, H.J. Smith, S.J. Burke, Information privacy: corporate management and national regulation, Organization Science 11 (1) (2000) 35–57.
[47] G.R. Milne, M.J. Culnan, H. Greene, A longitudinal assessment of online privacy notice readability, Journal of Public Policy & Marketing 25 (2) (2006) 238–249.
[48] A.D. Miyazaki, Online privacy and the disclosure of cookie use: effects on consumer trust and anticipated patronage, Journal of Public Policy & Marketing 27 (1) (2008) 19–33.
[49] Z. Papacharissi, J. Fernback, Online privacy and consumer protection: an analysis of portal privacy statements, Journal of Broadcasting & Electronic Media 49 (3) (2005) 259–281.
[50] P.A. Pavlou, State of the information privacy literature: where are we now and where should we go? MIS Quarterly 35 (4) (2011) 977–988.
[51] P.A. Pavlou, H. Liang, Y. Xue, Understanding and mitigating uncertainty in online exchange relationships: a principal-agent perspective, MIS Quarterly 31 (1) (2007) 105–136.
[52] S.S. Petronio, Communication boundary management: a theoretical model of managing disclosure of private information between marital couples, Communication Theory (1991) 311–335.
[53] S.S. Petronio, Boundaries of Privacy: Dialectics of Disclosure, State University of New York Press, Albany, NY, 2002.
[54] P.M. Podsakoff, S.B. MacKenzie, J.Y. Lee, N.P. Podsakoff, Common method biases in behavioral research: a critical review of the literature and recommended remedies, Journal of Applied Psychology 88 (5) (2003) 879–903.
[55] A.D. Rensel, J.M. Abbas, H.R. Rao, Private transactions in public places: an exploration of the impact of the computer environment on public transactional web site use, Journal of the Association for Information Systems 7 (1) (2006) 19–51.
[56] A. Riahi-Belkaoui, E. Pavlik, Accounting for Corporate Reputation, Quorum Books, Westport, CT, 1992.
[57] C.M. Ringle, S. Wende, S. Will, SmartPLS 2.0 (M3) Beta, http://www.smartpls.de 2005 (Hamburg).
[58] A.J. Rohm, G.R. Milne, Just what the doctor ordered: the role of information sensitivity and trust in reducing medical information privacy concern, Journal of Business Research 57 (9) (2004) 1000–1011.
[59] R. Rust, P. Kannan, N. Peng, The customer economics of internet privacy, Journal of the Academy of Marketing Science 30 (4) (2002) 455–464.
[60] Y. Sai, Transparent Safe, Decision Support Systems 46 (1) (2008) 41–51.
[61] H.J. Smith, T. Dinev, H. Xu, Information privacy research: an interdisciplinary review, MIS Quarterly 35 (4) (2011) 989–1015.
[62] J.Y. Son, S.S. Kim, Internet users' information privacy-protective responses: a taxonomy and a nomological model, MIS Quarterly 32 (3) (2008) 503–529.
[63] T.F. Stafford, A. Urbaczewski, Spyware: the ghost in the machine, Communications of the Association for Information Systems 14 (15) (2004) 291–306.
[64] C. Van Slyke, J.T. Shim, R. Johnson, J. Jiang, Concern for information privacy and online consumer purchasing, Journal of the Association for Information Systems 7 (6) (2006) 415–443.
[65] A.F. Westin, Privacy and Freedom, Athenaeum, New York, 1967.
[66] A.F. Westin, Social and political dimensions of privacy, Journal of Social Issues 59 (2) (2003) 431–453.
[67] W. Wood, Attitude change: persuasion and social influence, Annual Review of Psychology 51 (1) (2000) 539.
[68] H. Xu, R.E. Crossler, F. Bélanger, A value sensitive design investigation of privacy enhancing tools in web browsers, Decision Support Systems (0) (2012).
[69] H. Xu, T. Dinev, H.J. Smith, P. Hart, Information privacy concerns: linking individual perceptions with institutional privacy assurances, Journal of the Association for Information Systems 12 (12) (2011) 798–824.
[70] M.Z. Yao, R.E. Rice, K. Wallis, Predicting user concerns about online privacy, Journal of the American Society for Information Science & Technology 58 (5) (2007) 710–722.
[71] J.C. Zimmer, R. Arsal, M. Al-Marzouq, D. Moore, V. Grover, Knowing your customers: using a reciprocal relationship to enhance voluntary information disclosure, Decision Support Systems 48 (2) (2010) 395–406.
[72] M. Zviran, User's perspectives on privacy in web-based applications, Journal of Computer Information Systems 48 (4) (2008) 97–105.

Yuan Li is an associate professor of business in the Division of Business, Mathematics and Sciences at the Columbia College in Columbia, South Carolina, U.S.A. He received his Ph.D. in Management Information Systems from the University of South Carolina. His current research focuses on knowledge management at the organizational and individual levels, knowledge and skills transfer in end user computing, and online information privacy. His research appears in the *Journal of the Association for Information Systems*, *European Journal of Information Systems*, *Decision Support Systems*, the *Journal of Organizational and End User Computing*, and the *Communications of the Association for Information Systems*.