Decision Support Systems 51 (2011) 434–445

Contents lists available at ScienceDirect

Decision Support Systems

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

The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors

Han Li [a,*], Rathindra Sarathy [b], Heng Xu [c]

[a] Minnesota State University Moorhead, USA
[b] Oklahoma State University, USA
[c] Pennsylvania State University, USA

ARTICLE INFO

Article history:
Received 5 February 2010
Received in revised form 3 October 2010
Accepted 29 January 2011
Available online 4 February 2011

Keywords:
Privacy belief
Privacy concern
Emotion
e-Commerce
Social contract

ABSTRACT

Based on the privacy calculus framework and the stimulus–organism–response (S–O–R) model, this study examines online information disclosure decision as a result of affective and cognitive reactions of online consumers over several stages, i.e. an initial stage where an overall impression is formed about an unfamiliar online vendor, and a subsequent information exchange stage where information necessary to complete the ecommerce transaction will be provided to the online vendor. We found that, initial emotions formed from an overall impression of a Web site act as initial hurdles to information disclosure. Once online consumers enter the information exchange stage, fairness-based levers further adjust privacy beliefs.

1. Introduction

Online consumers are facing serious threats to their information privacy. The ubiquitous connectivity of the wired and wireless network platform supporting e-commerce has led to an expansion in the sources of data and easier access to personal information. A number of reputable firms such as Google [35,36] and Facebook [60] have faced privacy-related backlashes in recent years. For instance, Amazon.com has been criticized for exercising price discrimination using personal information that they collected [16]. In a recent study analyzing the current state of Web privacy practices [33], it was found that reputable e-commerce websites like eBay, Amazon, and Paypal share their collected customer data with hundreds of their affiliated companies.

As vast amounts of personal information is being exchanged, stored and shared, individual privacy is under public scrutiny. Recent studies have shown that information privacy is considered to be one of the major obstacles to the growth of e-commerce [34,57]. Most online consumers have refused to provide their personal information at one time or another and a large percentage of them have falsified personal information provided to online vendors [61]. It has been shown that more than half of the consumers (61%) were hesitant to disclose credit card information online [29]. Clearly, understanding factors influencing an online consumer's willingness to provide personal information is important to both online vendors and the growth of e-commerce.

A large body of research has focused on consumers' general privacy concern [22,45,56–58,65], which is defined as an individual's general tendency to worry about information privacy [45]. General privacy concern is not specific to a particular context (e.g., a specific Web site or online company) and differs from person to person. Empirical studies examining general privacy concern have been inconsistent in terms of its role in influencing privacy-related beliefs or behavior [10,22,45,56,58]. General privacy concern was found to be significant when included as a sole predictor of privacy-related behavior [56,58] but was found to have a weak or insignificant impact in the presence of other variables such as trust belief, risk belief, etc. [3,37,45].

These inconsistent findings compel us to reexamine the nature of general privacy concern and its role in influencing privacy decision-making. One possible explanation for these inconsistent findings is that the effect of general privacy concern may be overridden by situational factors, i.e. factors related to a specific Web site or online company [63]. Emphasizing the role of situation-specific factors in shaping privacy beliefs, Laufer and Wolfe [39] suggest that individuals form their privacy beliefs by evaluating concrete situational elements such as features of the physical space, institutional definition of appropriate behavior, expected risks and benefits, etc. General privacy concern has been found to be fully mediated by those situational trust and risk beliefs formed from the direct interaction with a specific Web site [63]. This is consistent with the idea that: "Individuals' concepts of privacy are tied to concrete situations in everyday life" [39]. Therefore,

* Corresponding author.
E-mail address: li@mnstate.edu (H. Li).

0167-9236/$ – see front matter
doi:10.1016/j.dss.2011.01.017

in this research, we aim to respond to the recent call for examining privacy decision-making taking into account situation-specific factors [45,57,63]. Our conjecture is that antecedents of online privacy decisions must encompass situational factors at a specific level.

To explore the situational factors that influence an individual's online privacy decision-making, we use the privacy calculus framework and the stimulus–organism–response (S–O–R) model to identify both affect-based and cognition-based factors in order to determine the circumstances under which people modify their willingness to provide personal information online. We treat the ecommerce transaction as consisting of i) an initial stage where an overall impression is formed about the Web site of an unfamiliar online vendor, and ii) a subsequent information exchange stage where information necessary to complete the ecommerce transaction will be provided to the online vendor. More specifically, we theorize how initial emotions formed from an overall Web site impression influence privacy-related beliefs (*affective* lens) and how exchange fairness influences privacy-related beliefs (*cognitive* lens). While emotions may be formed throughout the interaction with an online vendor's Web site, we study whether initial emotions formed from an early impression of the vendor's Web site impact privacy beliefs.

Our findings suggest that online consumers' initial emotions and later-stage exchange fairness levers do indeed jointly determine their privacy beliefs that, in turn, drive their intention to disclose personal information. In comparison, general privacy concern was found to be a far less important factor influencing privacy beliefs and behaviors. The results not only provide important insights into resolving some of the equivocation found in the literature regarding privacy behavior, but also better explain inconsistencies in consumers' privacy behavior found in practice. Overall, we contribute to theory by examining the situation-specific individual privacy decision-making process in order to understand several stages of privacy decision formation in a structured nomological net.

2. Theoretical foundation

2.1. Privacy calculus

A consumer's decision to disclose personal information is based on a cost–benefit analysis or the so-called "privacy calculus" [22,37,39]. Individuals consider the merits and potential negative consequences with respect to the current interaction as well as future situations. Since the online consumer acts on beliefs and dispositions rather than solely on known costs and benefits, these beliefs factor into the privacy-related cost-benefit analysis. In this study, two types of privacy beliefs are investigated: *privacy protection belief* and *privacy risk belief*. Privacy protection belief refers to the subjective probability that consumers believe that a specific online vendor will protect their private information as expected [38,48,51]. Privacy risk belief is defined as the expected loss potential associated with releasing personal information to a specific firm [40,45]. These two privacy beliefs, although related, represent two separate aspects of information privacy assessment. When an online consumer believes that the vendor will protect his/her information from potential privacy harms, such belief (privacy protection belief) acts as a benefit factor in the privacy calculus. On the other hand, privacy risk is treated by the consumer as a cost factor with privacy risk belief adding to the cost in the privacy calculus. Therefore, in this study, privacy protection belief and privacy risk belief are treated separately as benefit belief and cost belief in the cost–benefit analysis involved in the privacy calculus governing information disclosure.

Information disclosure is dependent upon the favorable assessments of both the level of privacy protection offered and the extent of privacy risks, i.e. high protection *and* low risk. Further, these two privacy beliefs may be driven or shaped by different factors and they may also play different roles in influencing privacy decisions or behaviors. For example, the collection of highly sensitive personal data is more likely to influence privacy risk belief instead of privacy protection belief.

In summary, individuals engage in a decision process to weigh the costs and benefits associated with disclosing information. Although such a calculus perspective of privacy has widely received attention within the IS field, no single study has combined both affect-based and cognition-based factors that can determine the circumstances under which people modify the situation-specific privacy calculus. As we argued earlier, the contextual nature of individual privacy decision making suggests that investigations of privacy must pay attention to salient beliefs and contextual differences at a specific level. We next describe literature associated with the stimulus–organism–response (S–O–R) model to help characterize a setting in which both affect-based and cognition-based factors are likely to play a role in a situation-specific privacy calculus.

2.2. Affective and cognitive reactions

Privacy-related decision-making processes are dynamic, varying with situational factors [22,39]. When online consumers interact with a specific Web site, they experience various situational factors such as characteristics of the Web site, their affective and cognitive reactions resulting from the interactions with the Web site, etc. Considering the situation-specific nature of privacy behaviors, we adopted the stimulus–organism–response (S–O–R) model in environmental psychology as the overarching theory to understand the formation of affective and cognitive reactions of online consumers and their impacts on privacy behaviors. The S–O–R model posits that environmental cues (i.e., stimuli) influence an individual's affective and cognitive reactions (i.e., internal states of organism), which further affect behavior (i.e., responses) [46]. The model has been applied by Parboteeah et al. [50] to explain online consumers' impulse purchasing behaviors as a consequence of cognitive and affective reactions to Web site characteristics.

The use of S–O–R model is appropriate in this study for two reasons. First, S–O–R centers on the reactions of the organism and the resulting behavioral responses when the organism is exposed to various situation specific environmental stimuli. As privacy behaviors are malleable with situational stimuli, the S–O–R model gives us a better understanding of how situational specific reactions influence privacy decision making. In addition, it allows us to integrate both affective and cognitive theoretical lenses and propose that privacy decision making is a result of both affective and cognitive reactions to a Web site.

Applying the S–O–R model to the online privacy context, environmental stimuli are various Web site characteristics, such as the overall look of the Web site, the types of information collected by the Web site, the presence of privacy policy on the Web site, among others. We argue that when online consumers interact with a Web site, those stimuli will generate both affective and cognitive reactions. In our research model, consumers' affective reactions are mapped as their emotional responses (i.e. joy and fear) to a Web site's overall look. Consumers' cognitive reactions are mapped as their privacy beliefs and appraisals about the Web site's privacy practices reflected by the sensitivity and relevance of information collected from them, as well as the privacy policy. These situational reactions are likely to influence privacy decision making process and possibly override the effect of general privacy concern on privacy behaviors. Further, to separate the effect of emotional and cognitive reactions, we examined initial emotional reactions to the overall look of the Web site occurring before information exchange, and cognitive reactions occurring during information exchange at a later stage of the Web site interaction. In the following subsections, we discuss the affective and cognitive lenses underlying our research model, define various constructs used in the study and review related literature.

2.2.1. Emotions as information

Much of the privacy research to-date [22,57] is based on the tradition that in privacy decision making, people conduct a cost–benefit analysis of the possible outcomes of alternatives to arrive at a decision. However, it is also well documented that emotions have the capacity to alter perceptions, physiology and abilities [18], which can also influence decision making.

"The notion that emotions determine beliefs was a common assumption during much of human history, and probably still is." [31, p.2]. Various informational theories have been introduced to explain how affect may influence people's thinking, judgment and decisions such as the affect-as-information model. The affect-as-information model "assumes that emotional feelings serve as affective feedback that guides judgment, decision making, and information processing" [15, p124]. Emotions could create emotion-congruent beliefs "by guiding attention to observable data" that match those emotions [14, p34]. So, individuals in negative emotional states may be more likely to seek negative evidence that confirms their emotions and vice versa.

In the psychology and IS literature, emotions have been empirically found to influence trust and risk perceptions in a *congruent* manner. For example, "happiness and gratitude – emotions with positive valence – increase trust. Anger – an emotion with negative valence – decreases trust" [25, p. 736]. Positive emotions toward a product or service help to reduce the perceived risks in using the product or service while negative emotions enhance the perceived risks [11]. Enjoyment has been found to increase individuals' perceived usefulness (PU) and perceived ease of use (PEOU) of information technology [66] while computer anxiety is confirmed to negatively influence PU [9] and PEOU [64].

In the privacy context, we argue that emotions may provide important feedback about the privacy characters of a Web site and shape the privacy beliefs of an individual. People may feel that some Web sites better fit their disposition to privacy than other Web sites. It has been found that a physical space could achieve its privacy character by design, activity, and meaning [39]. Similarly, a Web site could achieve its privacy character through design, content and functionality. For example, a visually appealing and professional Web site may trigger joy, while a poorly designed Web site may trigger frustration and/or fear. These emotions triggered by a Web site may be used by an individual as cues to evaluate the benefits or potential privacy risks and can shape beliefs in a congruent manner. The role of emotions is especially important for unfamiliar Web sites, where consumers have limited information to judge the privacy-related protections and risks offered by the Web site. Therefore, we argue that it is necessary to consider the effect of emotions to understand the formation of online consumers' privacy beliefs.

In this study, we focused on the impact of discrete basic emotions as they are considered to be innate and universal across cultures [54]. Shaver et al. [55] identified five basic emotions: love, joy, anger, sadness and fear. Considering the context of our study, we omitted love, anger and sadness.

Love is a type of interpersonal emotion, making it less suitable for emotional reactions to a Web site. Anger and sadness often occur when one has received some negative outcomes such as failed service or product, etc. For initial Web site interaction (before information and product exchange), sadness and anger should be less common. Therefore, we investigated the impacts of initial joy and fear triggered by overall Web site impression before information exchange.

2.2.2. Information exchange as a fair social contract

In addition to the initial emotional reactions to a Web site, online consumers will also have privacy-related cognitive reactions when they enter the stage of information exchange with the vendor at a later time during an ecommerce transaction. The privacy-related cognitive reactions could involve the appraisals of privacy policy, and the nature of information collected and the resulting privacy beliefs. Several studies have pointed out that personal information exchange is governed by a fair social contract [21,45]. A social contract is often required to govern the exchange process when the exchange involves unknown consequences, The underlying assumption of a social contract is bounded by moral rationality, i.e. "individual moral agents lack the information, time, and emotional strength to make perfect judgments" [23,24]. Information exchange in online shopping is often considered to be quite unpredictable. Once online consumers disclose their personal information to an online firm, the subsequent use of their personal information is often beyond their control. Therefore, based on the assumption of the social contract, a cognitive lens based on the social contract is appropriate for our research context, i.e. information exchange with an *unfamiliar* online vendor's Web site.

A social contract governing information exchange is formed based on the shared *understanding* or norms about the exchange process and outcomes [24]. One such shared norm is the expectation about costs and benefits of the information disclosure. Consumers tend to participate in the social contract as long as the perceived benefits exceed the costs [19]. Before disclosing personal information, consumers evaluate the benefits of disclosure against costs. To this end, the social contract governing information disclosure involves a cost–benefit analysis.

In addition, for an information exchange, the norms associated with the social contract also entail shared understanding about exchange fairness [21,42], which has been operationalized as the fair information practice principles or FIP principles [21,49]. Exchange fairness as captured by FIP principles is the basis of a *fair social contract* governing the disclosure of personal information [21]. FIP principles are "procedures that provide individuals with control over the disclosure and subsequent use of their personal information and govern the interpersonal treatment that consumers receive" [21, P.330].

Consumers further adjust their perceptions of costs and benefits based on the perceived fairness of a company's information practices [6]. The implementation of FIP principles could help to alleviate consumers' privacy concerns toward direct marketing or reduce their perceived privacy risks [19]. FIP principles provide a signaling function to consumers about risks in the exchange [21] and adjust the perceived costs and/or benefits in the privacy-related cost–benefit analysis. Low fairness will alert online consumers about potential risks involved in information exchange while fairness helps assuage consumers' risk perceptions. The adjustment by fairness of information exchange or FIP principles is especially important for unfamiliar Web sites where consumers could simultaneously perceive high benefits and high costs due to the uncertainty in the exchange. To this end, the fair social contract governing information exchange consists of a cost–benefit analysis adjusted by exchange fairness or FIP principles. FIP principles influence online consumers' privacy-related cost and benefit beliefs that, in turn, affect their information disclosure intention.

To examine information exchange as a fair social contract, we followed the FIP principles suggested in prior studies [21,49] and identified three fairness-based levers indicative of FIP principles of an online vendor. They are sensitivity and relevance of information collected, and awareness of privacy policy. These fairness levers are examined as antecedents adjusting privacy-related cost and benefit beliefs. Detailed discussions on each of these three levers and their effect on privacy beliefs are provided later in separate subsections.

3. Research model

Drawing from the literature summarized above, Fig. 1 depicts our conceptualization of the drivers of individuals' intentions to disclose personal information online. Our research model proposes that: (a) the initial emotional reactions to a specific vendor's Web site (*before* information exchange) and fairness-based levers employed by the vendor (*during* information exchange) jointly drive the user's privacy-related beliefs about the Web site or vendor; and (b) these

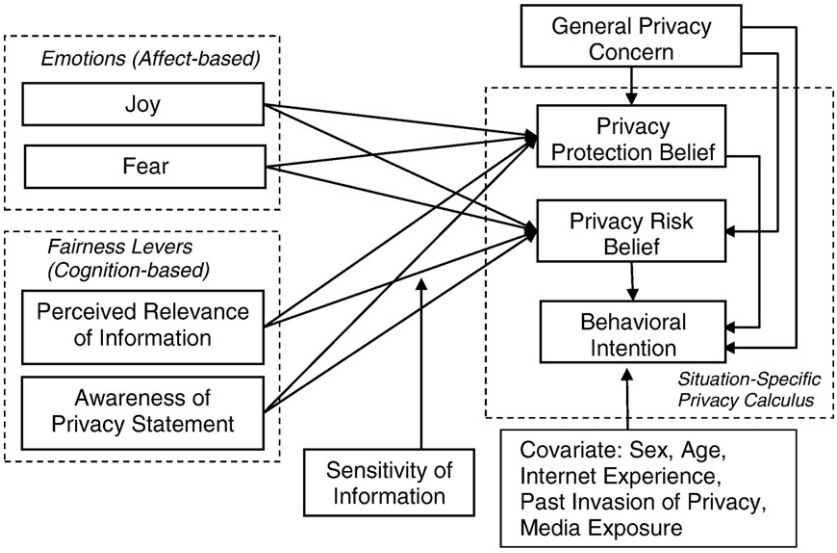

Fig. 1. Research model.

beliefs have a salient effect on behavioral intention to disclose personal information by impacting the privacy calculus. Fig. 1 shows the proposed hypotheses and Table 1 summarizes some of the core concepts underlying our research model.

3.1. Initial emotions and privacy beliefs

As discussed in the earlier section, affect tends to produce a congruent effect on people's thinking, judgment and decision [7,15,27]. Emotions can influence people's thinking and judgment in a way such that positive emotions tend to lead to more positive thinking or judgment than negative emotions. Personal cognitive beliefs (such as privacy beliefs) are essentially about *how* we think and, therefore, are expected to be influenced by emotions in a congruent way. At the same time, emotions and cognitive beliefs can be interdependent. Emotions are likely to vary in different stages of the interaction between online consumers and the Web site. Initial emotions formed from an overall Web site impression before information exchange may be different from those experienced at a later stage when online consumers are evaluating the information exchange based on the cost, benefit and perceived fairness of a social contract.

In this study, *we focused on the effect of initial emotions* and are interested in whether the effects of initial emotional reactions to overall Web site impression persist even through later stage cognitive processing that is necessary for information exchange. In other words, do the initial emotions continue to impact privacy beliefs even when consumers are immersed in information exchange? Dinev and Hart [22] were the first to model the influence of personal interest in the privacy calculus model. Their findings suggest that personal interest in Internet content can override concerns over providing personal information [22]. However, they also point out that future research is necessary to further explore the influence of personal interest in more specific contexts. To the degree that an individual's initial joy reflects their own personal interest in the content or service, we expect it to influence the situation-specific privacy calculus. Negative emotions such as fear can inform individuals that a situation is problematic (Petty, DeSteno, & Rucker, 2001) and, therefore, could also have an impact on the situation-specific privacy calculus. A considerable number of studies in psychology and IS have empirically found the congruent effect of emotions on individual beliefs [9,11,25,64,66] such that people in a positive emotions tend to have more positive beliefs than people in a negative emotion. Therefore, the initial joy and fear are expected to influence the two privacy beliefs in a congruent manner. We have:

H1. Initial joy has a positive effect on privacy protection belief.

H2. Initial joy has a negative effect on privacy risk belief.

H3. Initial fear has a negative effect on privacy protection belief.

H4. Initial fear has a positive effect on privacy risk belief.

3.2. Fairness levers and privacy beliefs

This subsection investigates three fairness levers (sensitivity and perceived relevance of information collected and awareness of

Table 1
Core concepts of the research model and their definitions.

Core concept	Acronym	Definition
Behavioral intention	BI	Willingness to provide personal information to a specific vendor to complete online transactions.
General privacy concern	PC	An individual's general tendency to worry about information privacy.
Joy	JOY	An emotional state of pleasure
Fear	FEAR	An emotional state of anxiety
Privacy risk belief	PRB	The expected loss potential associated with releasing personal information to a specific firm.
Privacy protection belief	PPB	The subjective probability that consumers believe that a specific online vendor will protect their private information as expected.
Perceived relevance of information	RELEV	The degree to which the data requested appears relevant or appear to have a bearing upon the purpose of the inquiry [59].
Awareness of privacy statement	APS	An individual's awareness of the content in the privacy statement of a Web site.
Information sensitivity	IS	The level of discomfort an individual perceives when disclosing a specific piece of information to a Web site.
Stimulus–Organism–Response	S–O–R model	Environmental cues (i.e., stimuli) influence an individual's affective and cognitive reactions, which further affect behavior (i.e., responses).
Fair information practice principles	FIP	Procedures that provide individuals with control over the disclosure and subsequent use of their personal information and govern the interpersonal treatment that consumers receive.

privacy policy) and their impact on the privacy-related cost–benefit beliefs, i.e. privacy protection belief and privacy risk belief. We are aware that the selection of these factors does not represent an exhaustive list of consumers' cognitive reactions. However, these three fairness levers reflect consumers' appraisals about privacy cues including both information cues and policy cues that a Web site may implement to reassure consumers about their efforts to protect consumers' personal information.

3.2.1. Sensitivity and relevance of information requested

In the literature [2,41], information sensitivity has been conceptualized as an attribute of personal information that informs the level of discomfort an individual perceives when disclosing that specific personal information to a specific Web site. The nature of information requested by a Web site could influence the privacy calculus through its level of sensitivity and legitimacy relative to the purpose of exchange. Not all types of information cause privacy-related worries. Consumers generally have little concern about providing basic demographic information (e.g. sex, age, education, marital status) and are slightly to moderately protective of information about their purchasing behavior, hobbies, occupation, name, email, postal address, and mostly concerned with the control over telephone numbers and financial information [32,48]. Disclosure of personal information inevitably implies the potential loss of control or risk of personal information. This is likely to increase privacy risk belief and the effect tends to be greater for more sensitive personal information.

At the same time, it is well recognized that there is no absolute privacy. The type of information such as its sensitivity by itself cannot determine whether the level of privacy provided meets consumers' *expectations*. The influence of sensitivity of information is relative, varying with situations [52]. Whether consumers will perceive certain types of requested information to be privacy invasive varies across the purpose of information collection. Information collection is less likely to raise negative privacy beliefs when information collected is relevant to the purpose of the transaction [49]. For example, the request for genetic testing data may not be considered to be invasive if the purpose is to provide medical advice. However, such information is likely to trigger strong privacy worries when requested by an insurance company. A consumer may worry that the information could be used to discriminate against her or him. Even the collection of low risk information such as gender in a context that is not relevant to the transactions may raise an alert about potential privacy risks in the future and the trustworthiness of the vendor. Privacy-related worries rise quickly when the type of information requested is perceived to have very low relevance, i.e. having little bearing on the purpose for which the data is collected. Therefore, this study focuses on the relevance of information and the potential moderating role of sensitivity on relevance. We propose:

H5. The perceived relevance of information requested has a positive impact on privacy protection belief.

H6. The perceived relevance of information requested has a negative impact on privacy risk belief.

H7. The effect of perceived relevance on privacy risk belief is moderated by sensitivity such that the effect is greater when sensitive information is requested.

3.2.2. Awareness of privacy policies on the web site

Privacy policies are widely adopted by vendors to address privacy concerns of online consumers [47]. A privacy policy is essentially a self-regulated organizational mechanism where consumers can be informed about the choices available to them regarding what is collected, how the collected information is used, the safeguards in place to protect the information from loss, misuse, or alteration, and how consumers can update or correct any inaccurate information. Online companies are responsible for protecting the information by implementing privacy policies based on the four basic elements of fair information practices: notice, choice, access and security [20]. Privacy literature suggests that an online firm's collection of personal information is perceived to be fair when the consumer is vested with notice and voice [20,45]. A privacy policy containing the four elements of FIP principles is meant to assure individuals about their control over the disclosure and subsequent use of their personal information [21]. It helps to increase the transparency of information collection procedures and help consumers evaluate the level of privacy protection offered by a Web site [47] and therefore decide whether to disclose information [37]. Hence, we propose that when a consumer is aware that a Web site implements a privacy policy manifesting fair information practices, it should help to increase his/her privacy protection belief and reduce privacy risk belief.

H8. Awareness of the privacy statement manifesting fair information practices has a positive impact on privacy protection belief.

H9. Awareness of the privacy statement manifesting fair information practices has a negative impact on privacy risk belief.

3.3. General privacy concern and privacy beliefs/behaviors

The general tendency to worry about information privacy (or general privacy concern) may also play a role in influencing online consumers' privacy beliefs and behaviors. General privacy concern, as an *individual's general tendency to worry about information privacy* [45], is not specific to a particular Web site or online company. It can differ among individuals and its impact on privacy behavior may be adjusted by environmental factors [62]. In the context of interaction with an unfamiliar Web site, online consumers often lack concrete information about the online vendor. General privacy concern, therefore, could play an important role in shaping consumers' privacy beliefs and directly impact their privacy behaviors. Some studies have found that privacy concerns reduce online consumers' intention to give out their personal information [56–58].Thus, we propose that general privacy concern will influence privacy protection belief and privacy behaviors negatively and privacy risk belief positively (i.e., increase perceived privacy risk).

H10. General privacy concern has a negative effect on privacy protection belief.

H11. General privacy concern has a positive effect on privacy risk belief.

H12. General privacy concern has a negative impact on online consumers' behavioral intention to disclose their personal information.

3.4. Privacy beliefs and behavioral intention to disclose personal information

In the trust and privacy literature, privacy decisions/behaviors have been studied by measuring the intention to purchase, give information, remove names from a direct marketing list, among others. This is in line with the research stream based on the theory of reasoned action (TRA) [26]. The same approach is taken by this study. We examine the effect of salient privacy beliefs on intention to release personal information. Consumers with a high privacy protection belief should perceive more control over the disclosure and subsequent use of their personal information, while those with high privacy risk beliefs are more likely to be wary about the potential loss of control over their personal information. Therefore,

H13. Privacy protection belief has a positive impact on online consumers' behavioral intention to disclose their personal information.

H14. Privacy risk belief has a negative impact on online consumers' behavioral intention to disclose their personal information.

4. Research methodology

4.1. Study design and procedures

Experimental design was employed to test the research model. An experimental Web site was created to allow easy manipulation of sensitivity of information. Utilizing an experimental design also allows us to rule out or control the effect of store familiarity and reputation, since our research focus is on initial information exchange for unfamiliar Web sites. To ensure realism, the interfaces of the experimental Website closely mimic a real commercial Web site providing Internet fax service, MyFax (http://www.myfax.com). Moreover, to increase the realism of the task, each subject assumed the role of an online shopper seeking internet fax service for the purpose of sending resumes for job applications. The subjects were introduced to some of the advantages of Internet fax service over email for job application before interacting with the experimental Web site. For example, faxed documents generally gain more attention from recruiters. Also, unlike email attachments, which may be deleted due to fear of computer viruses, faxes are considered safer by recruiters.

The experimental web site has a 30-day free trial membership sign-up form, which was used to manipulate information sensitivity. The sensitivity of information was manipulated at two levels: low and high. A common set of information of low to moderate sensitivity that included name, gender, email, and postal address was requested for both low and high sensitivity treatment conditions. Besides the common information, the high sensitivity condition also had requests for telephone number and credit card information.

This study measured whether subjects read the privacy policy. Thus, privacy policy was not manipulated in the design. This is different from the approach taken in previous studies that have mainly examined the effect of availability and/or the level of guarantee of privacy policy through experimental manipulation. These studies randomly assign subjects to each treatment group which dictates whether the privacy policy has to be read or not. They mostly ignored "contextual factors relating to the likelihood that a privacy policy statement will be read" [47]. A perfect privacy policy will not be effective if nobody reads it. Several surveys have found that less than 50% of online consumers actually read privacy policies [1,47]. Therefore, to increase the realism of our research context, subjects in our study were free to decide whether to read the privacy policy or not. The privacy policy used in the experimental Web site was designed along the lines of a strong privacy policy, i.e. containing all basic elements of FIP principles.

Subjects were randomly assigned to only one of two treatment conditions, i.e. either low sensitivity or high sensitivity information requests. A major task page was used to introduce the task scenario to subjects and provide detailed step by step instructions. Subjects were required to interact with the experimental site as naturally as possible for about 10 min to get an overall impression of the Web site. Then, they were instructed to fill out section I of the survey that measured their initial emotions before information exchange. The next stage of the experiment simulated an information exchange context. Subjects were instructed to *evaluate* a sign-up form of the company's 30-day free trial program and made aware that they were not required to fill the form with their private information. A link to the vendor's privacy policy was provided at the bottom of the form. They could choose to read the privacy policy if they felt it was necessary. After evaluating the sign-up form, subjects were required to fill out the succeeding two sections of the survey.

4.2. Variable measurement

Existing published scales were adapted to measure variables in the research model whenever possible. Some items were re-worded slightly to reflect the research context. Joy and fear were measured by items developed by Shaver et al. [55]. Perceived relevance items were modified from Stone [59].

Privacy protection belief was measured using the scales by Pavlou and Chellappa [51]. Privacy risk belief was adapted from the instruments by Malhotra et al. [45]. Behavioral intention (to disclose personal information) was measured by scales after Malhotra et al. [45] and MacKenzie and Spreng [44]. General privacy concern consists of three items developed by Malhotra et al. [45] to tap global information privacy concern. The detailed general privacy concern scale developed by Malhotra et al. [45] was not used in this study because the focus of this study is not on the sub-dimensions of privacy concern. Two emotion constructs were measured using five-point Likert scales with 1 being "not at all" and 5 being "very much". All the remaining constructs were measured on seven-point Likert scales with 1 being "strongly disagree" and 7 being "strongly agree". The detailed scales for each latent construct are available in the Appendix. In addition, the survey consists of one binary scale question asking about whether the subject has read the privacy policy. We also developed one seven-point Likert scale question to check whether the manipulation on sensitivity is successful. The question inquires about how subjects perceive the level of sensitivity of the information in the 30-day free trial sign-up form.

4.3. Survey administration

Before the final experiment, a pilot study was administered to 20 undergraduate and graduate students at a major Midwestern U.S. university. The purpose was to identify and refine potentially ambiguous measurement items, and assess the clarity of survey instructions and the length of the time needed to complete the survey. In the final experimental study, the recruitment message was delivered in class to about 220 students who are different from those in the pilot study. The recruiting message informed the subjects that they were being recruited for a study examining online shopping. To increase the realism of the experiment, subjects were told that they would be requested to visit a commercial Web site and then complete a short paper-based survey. So, the subjects were not explicitly aware that they were interacting with an artificial Web site.

The participation was voluntary. Extra credit accounting for about 2% of their total grade was used as participation incentive. A total of 175 valid responses were received. About 50% of these respondents were part-time students with working experience. The demography of survey respondents shows an equal representation of male and female and a fairly wide distribution in age and Internet experience (Table 2).

4.4. Control variables

Five variables that might influence privacy decisions/behaviors were included in this study as control variables for predicting intention to disclose personal information. They are gender, age, Internet experience, previous experience of being victims of privacy invasion, and media exposure of privacy invasion incidents.

5. Data analysis

First, the result of manipulation of sensitivity of information was checked using an independent *t*-test. Perceived sensitivity for subjects assigned to the high sensitivity group was significantly higher than that of the low sensitivity group ($p<0.001$). Therefore, information sensitivity manipulation was successful. The research model was then tested with partial least squares (PLS) technique. PLS requires a much smaller sample size than other structural equation modeling (SEM) techniques. The minimum sample size requested by PLS is ten times the larger number of paths going to an endogenous construct when all

Table 2
Demography distribution of survey respondents.

Gender		Age	
Male	47.4%	19–25	77.7%
Female	52.6%	26–30	11.4%
		30–35	4.6%
Internet experience		36–40	2.9%
<1 year	6.9%	40–45	2.3%
1–3 year	24.7%	>45	1.1%
3–6 year	45.4%		
≥6 year	23.0%		

constructs are reflective [12]. For our research model, the maximum number of paths leading to an endogenous variable is eight, considering the control variables. Therefore, a sample size of 175 is sufficient for us to use PLS. Furthermore, PLS does not assume a multivariate normal distribution and interval scales, making it appropriate to test a research model with manipulated constructs like sensitivity.

5.1. Measurement model

To validate the measurement model, we tested reliability, convergent and discriminant validity of the latent constructs. A scale is considered reliable if its composite reliability (CR) is above 0.7 and average variance extracted (AVE) above 0.5 [4]. As shown in Table 3, all scales were found to be reliable. To establish convergent validity, all indicators of a latent construct should have loadings above 0.6 [4]. From Table 3, loadings of all items are above this recommended cutoff, suggesting convergent validity of all latent constructs. Discriminant validity of each latent construct was tested by the method recommended by Fornell and Larcker [28]. The square root of AVE of each construct should be higher than the correlation between that construct and any other constructs. This criterion is satisfied by all latent constructs (Table 4). Therefore, our measurement model exhibits sound reliability and validity necessary for further testing of the research hypotheses.

5.2. Hypotheses testing

Fig. 2 and Table 5 summarize the results of testing the hypotheses. In Fig. 2, completely standardized path coefficients are given on each significant path. The amount of variance explained in each endogenous variable (or R^2) is displayed within the corresponding construct rectangle. We hypothesized that emotions have a congruent effect on privacy beliefs. This congruent effect was supported. Joy is found to have a significant positive effect on privacy protection belief ($p<0.001$) and significant negative effect on privacy risk belief ($p<0.001$). Fear has a significant positive effect on privacy risk belief ($p<0.05$). The relationship between fear and privacy protection belief was not statistically significant.

Before testing the main effect of relevance of information on privacy risk belief, it is necessary to study the potential moderating effect of sensitivity. We followed the procedures proposed by Chin et al. [13]. The effect size of interaction (f^2) was computed to be 0.00 for predicting privacy risk belief, which is far less than the 0.02 cutoff for small effect size [17]. The result of bootstrap sampling also shows that the interaction effect was not significant. Therefore, sensitivity is not found to significantly moderate the relationship between information relevance and privacy risk belief. In the absence of a moderating effect, the main effects of relevance and sensitivity as the antecedents of privacy beliefs were tested. Relevance was found to have a significant positive impact on privacy protection belief ($p<0.001$) and negative impact on privacy risk belief ($p<0.001$). Sensitivity of information has no significant impact on privacy risk belief ($p>0.05$).

Table 3
Loadings/cross-loadings, composite reliability (CR) and average variance extracted (AVE) of measurement instruments.

Constructs/items		Loadings/cross-loadings						
		1	2	3	4	5	6	7
1. Joy	joy1	**0.94**	−0.09	0.21	0.37	−0.25	0.21	−0.03
CR = 0.958	joy2	**0.94**	−0.14	0.16	0.37	−0.29	0.25	−0.04
AVE = 0.883	joy3	**0.94**	−0.10	0.10	0.34	−0.26	0.22	−0.02
2. Fear	Fear1	0.03	**0.75**	−0.06	0.03	0.11	−0.05	−0.09
CR = 0.882	Fear2	−0.14	**0.93**	−0.16	−0.14	0.21	−0.21	−0.10
AVE = 0.715	Fear3	−0.12	**0.85**	−0.05	−0.07	0.17	−0.09	−0.09
3. Relevance of Infor	Relev1	0.20	−0.15	**0.91**	0.29	−0.37	0.47	−0.14
CR = 0.906	Relev2	0.10	−0.06	**0.79**	0.30	−0.26	0.29	−0.06
AVE = 0.764	Relev3	0.14	−0.10	**0.92**	0.34	−0.33	0.48	−0.16
4. Privacy Protection	PPB1	0.37	−0.14	0.24	**0.79**	−0.46	0.29	0.02
Belief	PPB2	0.26	−0.03	0.24	**0.71**	−0.39	0.26	−0.07
CR = 0.875	PPB3	0.32	−0.11	0.18	**0.82**	−0.47	0.30	0.01
AVE = 0.585	PPB4	0.25	−0.08	0.41	**0.80**	−0.54	0.47	−0.08
	PPB5	0.26	0.00	0.26	**0.69**	−0.38	0.22	0.02
5. Privacy Risk	PBR1	−0.23	0.15	−0.28	−0.56	**0.89**	−0.48	0.19
Belief								
CR = 0.950	PBR2	−0.27	0.13	−0.25	−0.49	**0.90**	−0.42	0.21
AVE = 0.827	PBR3	−0.29	0.24	−0.38	−0.58	**0.93**	−0.48	0.26
	PBR4	−0.24	0.21	−0.41	−0.52	**0.92**	−0.50	0.24
6. Behavioral	BI1	0.28	−0.14	0.44	0.40	−0.50	**0.93**	−0.26
Intention								
CR = 0.963	BI2	0.28	−0.14	0.44	0.41	−0.53	**0.96**	−0.27
AVE = 0.866	BI3	0.14	−0.13	0.43	0.36	−0.43	**0.91**	−0.25
	BI4	0.19	−0.19	0.47	0.38	−0.47	**0.92**	−0.26
7. Privacy Concern	PC1	0.04	−0.12	−0.09	−0.03	0.18	−0.22	**0.82**
CR = 0.866	PC2	0.01	−0.15	−0.14	0.05	0.13	−0.14	**0.79**
AVE = 0.683	PC3	−0.10	−0.04	−0.13	−0.06	0.26	−0.29	**0.87**

Awareness of the privacy policy demonstrating FIP principles was found to significantly enhance privacy protection belief ($p<0.05$) but was not significant in shaping privacy risk belief. Besides the above affect-based and cognition-based situational factors, general privacy concern had a significant influence on privacy risk belief ($p<0.001$) but was not significant for the formation of privacy protection belief. In all, the model can explain 25.3% of the variance in privacy protection belief and 25.9% of the variance in privacy risk belief.

The two privacy beliefs (protection belief and risk belief) and general privacy concern were further found to have a significant impact on behavioral intention to disclose personal information. No control variables were found to be significant. Overall the model could account for 33.7% variance of behavioral intention. The result also suggests that general privacy concern has a significant *direct* impact on behavioral intention *as well as* a significant *indirect* effect on behavioral intention through privacy risk belief.

6. Discussion

6.1. Summary of findings

The results of the experiment indicate that, for an unfamiliar Web site, privacy behaviors are driven by both general privacy concern and

Table 4
Discriminant validity of measurement model.

	Joy	Fear	Relev	PPB	PRB	BI	PC
Joy	**0.940**						
Fear	−0.119	**0.846**					
Relev	0.167	−0.119	**0.874**				
PPB	0.383	−0.100	0.356	**0.765**			
PRB	−0.282	0.205	−0.369	−0.596	**0.909**		
BI	0.242	−0.162	0.479	0.415	−0.519	**0.931**	
PC	−0.034	−0.109	−0.140	−0.030	0.248	−0.282	**0.826**

Note: Diagonal elements are the square root of the AVE values. Off-diagonal elements are the correlations among latent constructs.

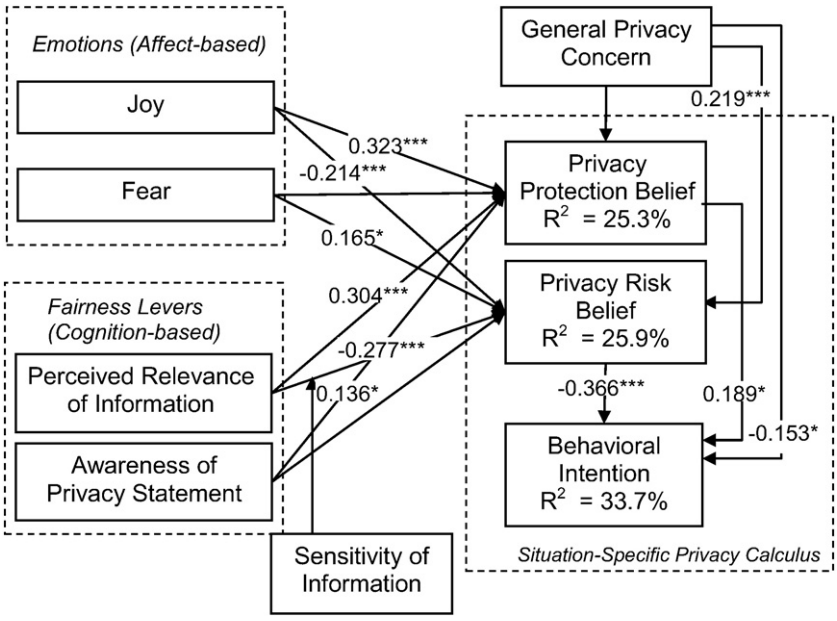

Fig. 2. Results of testing hypotheses using PLS analysis. Completely standardized estimates, controlled for covariates in the research model, *p<0.05, **p<0.01, ***p<0.001.

Table 5
Summary of hypothesis testing results.

Hypotheses	Path Coefficients	*t* Value	p value
H1 Initial joy has a positive effect on privacy protection belief.	0.323	5.71	p<0.001 (supported)
H2 Initial joy has a negative effect on privacy risk belief.	−0.214	3.39	p<0.001 (supported)
H3 Initial fear has a negative effect on privacy protection belief.	−0.020	0.27	p>0.05 (not supported)
H4 Initial fear has a positive effect on privacy risk belief.	0.165	2.74	p<0.01 (supported)
H5 The perceived relevance of information requested has a positive impact on privacy protection belief	0.304	4.86	p<0.001 (supported)
H6 The perceived relevance of information requested has a negative impact on privacy risk belief.	−0.277	3.77	p<0.001 (supported)
H7 The effect of perceived relevance on privacy risk belief is moderated by sensitivity such that the effect is greater when sensitive information is requested.	0.026	0.27	p>0.05 (not supported)
H8 Reading the privacy statement manifesting fair information practices has a positive impact on privacy protection belief.	0.136	2.12	p<0.05 (supported)
H9 Reading the privacy statement manifesting fair information practices has a negative impact on privacy risk belief.	0.034	0.47	p>0.05 (not supported)
H10 General privacy concern has a negative effect on privacy protection belief.	0.006	0.09	p>0.05 (not supported)
H11 General privacy concern has a positive effect on privacy risk belief.	0.219	3.43	p<0.001 (supported)
H12 General privacy concern has a negative impact on online consumers' behavioral intention to disclose their personal information.	−0.153	2.16	p<0.05 (supported)
H13 Privacy protection belief has a positive impact on online consumers' behavioral intention to disclose their personal information.	0.189	2.06	p<0.05 (supported)
H14 Privacy risk belief has a negative impact on online consumers' behavioral intention to disclose their personal information.	−0.366	3.47	p<0.001 (supported)

privacy-related cost–benefit beliefs. Privacy beliefs, in turn, are shaped by general privacy concern, initial emotions and fairness levers. Initial emotions formed from an overall impression of the Web site continue to play an important role in shaping privacy beliefs and decisions, even if subjects are exposed to cognitive processing of information exchange at a later time. Thus, *initial emotions have a lasting coloring effect on later stage cognitive processing.* Specifically, joy significantly enhances privacy protection belief and reduces privacy risk belief. Interestingly, fear was found to significantly influence privacy risk belief, but not impact privacy protection belief. This finding corroborates the broaden-and-build theory that posits that negative emotions narrow one's momentary thought–action repertoire [30]. As a result, being afraid would drive one into an escape or avoidance mode, preventing consumers from actively evaluating the potential level of privacy protection offered. Instead, they focus on the risks involved in the situation and reach a quick decision regarding the potential privacy risks of the Web sites, and act accordingly.

When online consumers enter the information exchange stage, fairness levers (relevance of information requested and privacy policies) were found to adjust privacy beliefs. As expected, perceived relevance of information requested was found to significantly increase privacy protection belief and reduce privacy risk belief. Although this finding is consistent with prior studies [37,59], to our knowledge this study is the first that empirically validated the impact of perceived relevance on privacy beliefs and, subsequently, privacy behaviors. The sensitivity of information was not found to be a significant fairness lever influencing privacy risk belief either directly or through the interaction with perceived relevance. An explanation may be that the effect of the sensitivity of information is fully overridden by that of perceived relevance as the influence of the sensitivity of information is relative and varies with the purpose of information collection.

Besides perceived relevance, awareness of the privacy policy incorporating FIP principles was found to be another significant fairness lever that enhances privacy protection belief. This finding is consistent with the study by Meinert et al. [47]. Surprisingly, awareness of the privacy policy does not significantly reduce privacy risk belief. This may be largely due to the self-commitment nature of a privacy policy, which outlines the level of privacy protection that a Web merchant promises to its consumers. For an unfamiliar Web site, such self-reported guarantee or a privacy policy may not effectively

reassure online consumers about the potential risks or unknown consequences of releasing personal information.

Finally, general privacy concern was found to significantly increase privacy risk belief and reduce online consumers' information disclosure intention. However, it has no significant impact on privacy protection belief. This finding is different from the study by Li et al. [43] in which general privacy concern increases privacy protection belief. One possible explanation for such different findings is that the effect of general privacy concern varies with different stages of the interaction between an online shopper and a Web site. The context of the study by Li et al. [43] was initial interaction before information exchange whereas this study covers both the initial interaction and the later information exchange stage. We conjecture that the effect of general privacy concern tends to decrease with progressive interaction with a Web site as more concrete information from the interaction could be based to assess the level of privacy protection offered by the online vendor. Therefore, in our study, the effect of general privacy concern on privacy protection belief may be overridden by that of initial emotions and fairness levers. As such, we further investigated the relative contributions of initial emotions, fairness-based levers (sensitivity and relevance of information collected and awareness of privacy policy) and general privacy concern. Three additional models were built by including only initial emotions, only fairness-based levers or only general privacy concern to predict privacy beliefs. The R^2 of these three alternative models were compared (Table 6). The results suggest that *emotions and fairness levers have about the same contribution in shaping the privacy beliefs and their effects dominate that of general privacy concern*.

We further checked the relative importance of the direct impact of general privacy concern on behavioral intention. An alternative model was built by excluding the direct path from general privacy concern to behavioral intention. Model R^2 decreases slightly from 33.7% to 31.9%, suggesting that situational beliefs are more important in influencing privacy decisions than general privacy concern. Therefore, when an online shopper is interacting with a Web site, his or her privacy beliefs are mainly influenced by situational emotions and fairness levers and his or her privacy beliefs that are formed (situation-specific) play a dominant role in driving his or her intention to disclose personal information. In this process, the effect of general privacy concern is far less important than these situational factors, i.e. emotions, fairness levers and privacy beliefs.

Overall, this research contributes to the privacy literature in e-commerce by integrating affective and cognitive situational factors at a specific level to understand dynamic formation of privacy beliefs and behaviors in a structured nomological net.

6.2. Research implications

The results of the study have several important implications for research on online information privacy. First, the use of S–O–R model as an overarching theory permits the examination of the effects of both affective and cognitive factors and their relationships at a specific level over and above that of general privacy concern. This study expands our understanding of factors influencing privacy beliefs and behaviors and helps to explain the weak, insignificant or even contradictory effect of privacy concerns on privacy behaviors reported in some of the prior studies [1,3,37,45,63]. As this study only examined a subset of situational factors at a specific level, future research could investigate other situational factors. For example, effort could be devoted to examining the effect of legislative and technical solutions on privacy decisions and the potential interactions among these solutions. It is possible that technical solutions are more effective in enhancing privacy protection belief while legislative solutions are more effective in reducing privacy risk belief. Interactions may also exist among situational factors. For example, fairness levers may moderate the effect of legislative and technical solutions.

Second, the findings in this study highlight the contextual nature of information sensitivity. The non-significant role of information sensitivity indicates that its effect is fully overridden by that of perceived relevance. That is to say, the influence of the sensitivity of information is relative and varies with the purpose of information collection. This has important implications for theoretical development since it opens a new avenue for the exploration of contextual nature of information sensitivity.

Third, we provide both theoretical and empirical support for the influence of initial emotions (affect) on privacy beliefs (cognition) even if online consumers were exposed to a later stage information exchange, suggesting that the initial emotions have a lasting impact. This builds and expands the recent growing body of IS research on the impact of affect on cognition and behaviors [5,9,11,43,64,66].

Fourth, the findings support the dynamic formation of privacy behaviors. It is important to consider the stage of interaction between an online shopper and an unfamiliar Web site. Drivers of privacy behaviors may vary at different stages of interaction between an online shopper and the Web site. Before any Web site interaction, general privacy concern may be the primary driver of online consumers' privacy behavior. With progressive Web site interaction, the effect of general privacy concern will be gradually mediated or overridden by specific emotional and cognitive reactions to the Web site. Specifically, during early interaction *before* information exchange, a good overall Web site impression is important for triggering positive emotions which, in turn, influence privacy beliefs and behaviors. During the later stage information exchange, fairness levers reflecting FIP principles act as another important set of drivers of privacy beliefs and behaviors. Future studies should consider the stage of the interaction with a Web site when examining online information privacy issues.

Fifth, the results of our study support the separation of privacy protection belief and privacy risk belief. Despite some common antecedents (joy and perceived relevance of information requested), these two beliefs are also driven by different situational factors. Future studies should separate these two privacy beliefs to gain more insights about mechanisms that are effective for enhancing the perceived level of privacy protection and/or reducing perceived privacy-related loss potential.

6.3. Managerial implications

Our study has several important practical implications for online vendors. First, our findings suggest that the effect of situational factors tends to override general privacy concern when consumers are interacting with a Web site. This may explain why the stated levels of privacy concerns of online consumers often deviate from their actual privacy decisions and behaviors.

Second, the longer lasting effect of initial emotions on privacy beliefs suggests that online vendors without established reputations need to pay special attention to the overall Web site design to engender favorable initial emotions formed based on the first impression of the Web site. For example, fear may be reduced if the site reflects a consumer's prototype of a highly reputable site. As stated by a recent New York Time article "reasoning comes later and is often guided by the emotions that preceded it" [8]. Favorable

Table 6
Comparison of relative explanatory power of initial emotions, fairness-based levers and privacy concern.

	R^2		
	Emotions only	Fairness levers Only	General privacy concern only
Privacy protection belief	15.2%	15.5%	0.1%
Privacy risk belief	10.9%	14.5%	6.1%

cognitive assessment of the privacy of a Web site does not form independent of a good Web site design. These initial emotions represent early hurdles that online vendors must overcome to attract online consumers into later-stage information disclosure supporting e-commerce transactions.

Third, information disclosure is influenced by privacy-related cost–benefit analysis, i.e. privacy protection belief and privacy risk belief. Online consumers assess both the level of privacy protection offered and potential privacy risks before disclosing their personal information. Online vendors should take measures to enhance privacy protection belief and reduce privacy risk belief. As suggested in this study, they could rely on fairness levers to adjust these two types of privacy belief. In particular, online vendors could post a privacy policy to notify consumers about their commitment to fair information practices, i.e. the level of privacy protection they offer. Another effective fairness lever identified in this study is relevance of information requested. The results of our study show that requesting relevant information increases privacy protection belief and reduces privacy risk belief. Therefore, online vendors need to be careful about what information to collect and ensure the information collected is legitimate or relevant to the purpose of the exchange.

6.4. Limitations and future research

Several limitations of this study should be recognized here. First, common method variance (CMV) might be a potential threat to the validity of our study. We attempted to reduce part of this threat by using an anonymous questionnaire and dividing the questionnaire into three sections with separate covers. Initial emotions before information exchange were measured in section I of the survey before subjects were exposed to the sign-up form of the Web site's 30-day free trial program, i.e. the simulated information exchange and subjects were required not to go back to the previous sections when they were filling later sections of the questionnaire. Harman's single-factor test was further used to assess the extent of common method variance [53]. All items belonging to the seven latent constructs were loaded simultaneously into an exploratory factor analysis, which yields a seven-factor solution. This suggests that common method variance is not a major problem. To further reduce the threat of common method variance, future studies could use different methods to measure independent and dependent variables. For example, intention to give personal information could be replaced with the measurement of actual privacy behaviors.

Furthermore, our studies only examined the effect of two privacy beliefs in driving privacy decisions. Other beliefs may compete with these two privacy beliefs. Future studies may focus on how privacy decisions are driven by other economic or non-economic benefits and related beliefs. For example, the perceived usefulness of the product or service could be important for privacy decisions, especially for Web sites used for non-hedonic purposes. Additional research is also needed to explore the impact of economic compensation on the privacy calculus and the potential interaction with fairness levers. From the perspective of social contract, fairness levers such as relevance of information are very likely to moderate the impact of economic benefits on privacy decisions.

Finally, this study used online shoppers' information disclosure intention as a surrogate for their actual privacy behavior. Although information disclosure intention has been verified to strongly predict actual disclosure behavior [67], future studies could be conducted to test the potential direct effects of emotions and fairness-based information levers on actual privacy behaviors.

7. Conclusions

Information privacy is a source of a growing tension between online firms and consumers. This study focused on unfamiliar Web sites and identified two sets of important situational factors (initial emotions and fairness levers) influencing consumers' privacy beliefs and decisions. The results of our study suggest that, initial emotions (joy and fear) formed based on overall Web site impression act as initial hurdles of information disclosure and were found to have a lasting coloring effect on later stage cognitive processing or the formation of salient privacy beliefs. Once online consumers enter information exchange stage, fairness-based levers (awareness of privacy policy and relevance of information) further adjust privacy protection belief and privacy risk belief.

Appendix. Survey instrument

Joy [55]	
Joy1	Joy
Joy2	Enjoyment
Joy3	Pleasure
Fear [55]	
Fear1	Fear
Fear2	Uneasiness
Fear3	Anxiety
Perceived relevance of information [59]	
Relev1	Information gathered seemed relevant for signing up for the 30-day free trial program
Relev2	Questions in the signup form appeared to have a bearing upon the purpose of the signing up.
Relev3	Information collected in the signup form look appropriate for signing up the free-trial program.
Privacy protection belief [51]	
PB1	I am confident that I know all the parties who would collect information if I transact with this vendor.
PB2	I am aware of the exact nature of information that will be collected during a transaction with this vendor.
PB3	I believe I have control over how my information will be used by this vendor if I transact with this vendor.
PB4	I believe I can subsequently verify the information I provide during a transaction with this vendor.
PB5	I believe there is an effective mechanism to address any violation of the information I provide to this vendor.
Privacy risk belief [45]	
PRB1	It would be risky to disclose my personal information to this vendor.
PRB2	There would be high potential for loss associated with disclosing my personal information to this vendor.
PRB3	There would be too much uncertainty associated with giving my personal information to this vendor.
PRB4	Providing this vendor with my personal information would involve many unexpected problems.
Behavioral intention to give personal information [45]	
Please specify the extent to which you would reveal your personal information to this vendor.	
BI1	Unlikely/likely
BI2	Not probable/probable
BI3	Impossible/possible
BI4	Unwilling/willing
General privacy concern [45]	
PC1	Compared to others, I am more sensitive about the way online companies handle my personal information.
PC2	To me, it is most important to keep my privacy intact from online companies.
PC3	I am concerned about threats to my personal privacy today.

References

[1] A. Acquisti, J. Grossklags, Privacy and rationality in individual decision making, IEEE Security & Privacy 3 (1) (2005).

[2] 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).
[3] 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).
[4] R.P. Bagozzi, Y. Yi, On the evaluation of structural equation models, Journal of the Academy of Marketing Science 16 (1) (1988).
[5] A. Bhattacherjee, Understanding information systems continuance: an expectation confirmation model, MIS Quarterly 25 (3) (2001).
[6] R.J. Bies, Privacy and procedural justice in organizations, Social Justice Research 6 (1993).
[7] G. H. Bower and J. P. Forgas, Mood and social memory Eds., Handbook of Affect and Social Cognition (Mahwah, NJ, Lawrence Erlbaum Associates, Inc, 2001).
[8] D. Brooks, The end of philosophy, in *The New York Times* (2009).
[9] M.J. Brosnan, Modeling technophobia: a case for word processing, Computers in Human Behavior 15 (1999).
[10] T. Buchanan, C. Paine, A.N. Joinson, U.-D. Reips, Development of measures of online privacy concern and protection for use on the Internet, Journal of the American Society for Information Science and Technology 58 (2) (2007).
[11] A. Chaudhuri, A study of emotion and reason in products and services, Journal of Consumer Behavior 1 (3) (2002).
[12] W.W. Chin, The partial least squares approach for structural equation modeling, in: G.A. Marcoulides (Ed.), Modern Methods for Business Research, Lawrence Erlbaum, Mahway, New Jersey, 1998.
[13] W.W. Chin, B.L. Marcolin, P.R. Newsted, A partial least squares latent variable modeling approach for measuring interaction effects: results from a Monte Carlo simulation study and an electronic mail adoption study, Information Systems Research 14 (2) (2003).
[14] G.I. Clore, K. Gasper, Feeling is believing: some affective influences on belief, in: N. H. Frijida, A.S.R. Manstead, S. Bem (Eds.), Emotions and Belief, University Press, Cambridge, 2000.
[15] G.L. Clore, K. Gasper, E. Garvin, Affect as information, in: J.P. Forgas (Ed.), Handbook of Affect and Social Cognition, Lawrence Erlbaum Associates, Inc, Mahwah, NJ, 2001.
[16] CNN.com, Web sites change prices based on customers' habits, http://www.cnn.com/2005/LAW/06/24/ramasastry.website.prices/, 2005.
[17] J. Cohen, Statistical Power Analysis for the Behavior Sciences, Hillsdale, NJ, Lawrence Erlbaum, 1988.
[18] L. Cosmides, J. Tooby, Evolutionary psychology and the emotions, in: M. Lewis, J.M. Haviland-Jones (Eds.), Handbook of Emotions, 2nd Ed, Guilford Press, New York, 2000.
[19] M.J. Culnan, P.K. Armstrong, Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation, Organization Science 10 (1) (1999).
[20] M.J. Culnan, J.R. Bies, Consumer privacy: balancing economic and justice considerations, Journal of Social Issues 59 (2) (2003).
[21] M.J. Culnan, R.J. Bies, Consumer privacy: balancing economic and justice consideration, Journal of Social Issues 59 (2) (2003).
[22] T. Dinev, P. Hart, An extended privacy calculus model for e-commerce transactions, Information Systems Research 17 (1) (2006).
[23] T. Donaldson, T.W. Dunfee, Toward a unified conception of business ethics: integrative social contracts theory, Academy of Management Review 19 (2) (1994).
[24] T.W. Dunfee, N.C. Smith, W.T. Ross, Social contracts and marketing ethics, Journal of Marketing Research 63 (July 1999).
[25] J.R. Dunn, M.E. Schweitzer, Feeling and believing: the influence of emotion on trust, Journal of Personality and Social Psychology 88 (5) (2005).
[26] M. Fishbein, I. Ajzen, Belief Attitude, Intention, and Behavior: An Introduction to Theory and Research, Addison-Wesley, Reading, MA., 1975
[27] J.P. Forgas, Affect, cognition, and interpersonal behavior: the mediating role of processing strategies, in: J.P. Forgas (Ed.), Handbook of affect and social cognition, Lawrence Erlbaum Associates, Mahwah, NJ, 2001.
[28] C. Fornell, D. Larcker, Evaluating structural equation models with unobservable variables and measurement error, Journal of Marketing Research 18 (1) (1981).
[29] Research Forrester, Consumers need education about privacy and security. 2009 (June 5th), http://www.forrester.com/Research/Document/Excerpt/0,7211,34441,00.html, 2004.
[30] B.L. Fredrickson, The role of positive emotions in positive psychology. The broaden-and-build theory of positive emotions, The American psychologist 56 (3) (2001).
[31] N.H. Frijda, A.S.R. Manstead, S. Bem, The influence of emotions on beliefs, in: N.H. Frijda, A.S.R. Manstead, S. Bem (Eds.), Emotions and Beliefs: How Feelings Influence Thoughts, Cambridge University Press, 2000.
[32] C. Gauzente, Web Merchants' privacy and security statements: how reassuring are they for consumers? A two-sided approach, Journal of Electronic Commerce Research 5 (3) (2004).
[33] J. Gomez, T. Pinnick, A. Soltani, Know privacy, 2009.
[34] I.-H. Hann, K.-L. Hui, S.-Y.T. Lee, I.P.L. Png, Overcoming online information privacy concerns: an information-processing theory approach, Journal of Management Information Systems 24 (2) (2007).
[35] S. Hansell, Google fights for the right to hide its privacy policy, NYtimes.com 2008.
[36] S. Hansell, Is google violating a California privacy law? NYtimes.com 2008.
[37] K.L. Hui, H.H. Teo, S.Y.T. Lee, The value of privacy assurance: an exploratory field experiment, MIS Quarterly 31 (1) (2007).
[38] 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).
[39] R.S. Laufer, M. Wolfe, Privacy as a concept and a social issue: a multidimensional development theory, Journal of Social Issues 33 (3) (1977).
[40] J. Lee, H.R. Rao, Perceived risks, counter-beliefs, and intentions to use anti-/counter-terrorism websites: an exploratory study of government-citizens online interactions in a turbulent environment, Decision Support Systems 43 (2007).
[41] X. Li, R. Santhanam, Will it be disclosure or fabrication of personal information? An examination of persuasion strategies on prospective employees, International Journal of Information Security and Privacy 29 (4) (2009).
[42] H. Li, R. Sarathy, Understanding online information disclosure as a privacy calculus adjusted by exchange fairness, 38th International Conference on Information Systems, (Montreal, Quebec, Canada, 2007), 2007.
[43] H. Li, R. Sarathy, J. Zhang, The role of emotions in shaping consumers' privacy beliefs about unfamiliar onlne vendors, Journal of Information Privacy and Security 4 (3) (2008).
[44] S.B. MacKenzie, R.A. Spreng, How does motivation moderate the impact of central and peripheral processing on brand attitudes and intentions? Journal of Consumer Research 18 (March 1992).
[45] 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).
[46] A. Mehrabian, J.A. Russell, An Approach to Environmental Psychology, MIT, Cambridge, MA, 1974.
[47] 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).
[48] M.J. Metzger, Privacy, trust, and disclosure: exploring barriers to electronic commerce, Journal of Computer-Mediated Communication 9 (4) (2004).
[49] Organization for Economic Cooperation and Development, Guidelines on the protection of privacy and transborder flows of personal data, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html, 1980.
[50] D.V. Parboteeah, J.S. Valacich, J.D. Wells, The influence of website characteristics on a consumer's urge to buy impulsively, Information Systems Research 20 (1) (2009).
[51] P.A. Pavlou, R.K. Chellappa, The Role of Perceived Privacy and Perceived Security in the Development of Trust in Electronic Commerce Transactions, Marshall School of Business, USC, Los Angeles, 2001.
[52] J. Phelps, G. Nowak, E. Ferrell, Privacy concerns and consumer willingness to provide personal information, Journal of Public Policy Marketing 19 (1) (2000).
[53] P.M. Podsakoff, S.B. MacKenzie, J.-Y. Lee, N.P. Podsakoff, Common method biases in behavior research: a critical review of the literature and recommended remedies, Journal of Applied Psychology 88 (5) (2003).
[54] M.J. Power, The structure of emotion: an empirical comparison of six models, Cognition & Emotion 20 (5) (2006).
[55] P. Shaver, J. Schwartz, D. Kirson, C. O'Connor, Emotion knowledge: further exploration of a prototype approach, Journal of Personality and Social Psychology 52 (6) (1987).
[56] H.J. Smith, S.J. Milberg, S.J. Burke, Information Privacy measuring individuals' concerns about organizational practices, MIS Quarterly 20 (2) (1996).
[57] J.-Y. Son, S.S. Kim, Internet users' information privacy-protective responses: a taxonomy and a nomological model, MIS Quarterly 32 (3) (2008).
[58] K.A. Stewart, A.H. Segars, An empirical examination of the concern for information privacy instrument, Information Systems Research 13 (1) (2002).
[59] D. L. Stone, The effects of the valence of outcomes for providing data and the perceived relevance of the data requested on privacy-related behaviors, beliefs and attitudes. vol. PhD Dissertation (1981).
[60] B. Stone and B. Stelter, Facebook Backtracks on Use Terms, in *The New York Times* (2009).
[61] M. Teltzrow, A. Kobsa, Impacts of user privacy preferences on personalized systems: a comparative study, in: C.M. Karat, J. Blom, J. Karat (Eds.), Designing Personalized User Experiences in eCommerce, Kluwer Academic Publishers, Dordrecht, Netherland, 2004.
[62] J.B. Thatcher, P.L. Perrewé, An empirical examination of individual traits as antecedents to computer anxiety and computer self-efficacy, MIS Quarterly 26 (4) (2002).
[63] 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).
[64] V. Venkatesh, Determinants of perceived ease of use: integrating control, intrinsic motivation, and emotion in the technology acceptance model, Information Systems Research 11 (4) (2000).
[65] M.Z. Yao, R.E. Rice, K. Wallis, Predicting user concerns about online privacy, Journal of the American Society for Information Science and Technology 58 (5) (2007).
[66] M.Y. Yi, Y. Hwang, Predicting the use of web-based information systems: self-efficacy, enjoyment, learning goal orientation, and the technology acceptance model, International Journal of Human-Computer Studies 59 (4) (2003).
[67] 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 (2010).

Han Li is currently an assistant professor in School of Business Administration at Minnesota State University Moorhead. She received her master's in Telecommunication Management, and doctorate in Management Information Systems from Oklahoma State University. She has published in *Decision Support Systems*, *Operations Research, Journal of Computer Information Systems, Information Management & Computer Security,* and *Journal of Information Privacy and Security*. Her current research interests include privacy and confidentiality, data and information security and the adoption of information technology.

Rathindra Sarathy is the Ardmore Professor of Business Administration in the Department of Management Science of Information Systems in the Spears School of Business at Oklahoma State University. He received his Ph.D. from Texas A&M University. He has published in many journals including *ACM Transactions on Database Systems*, *Decision Sciences*, *Decision Support Systems, Information Systems Research*, *Management Science*, and *Operations Research.* His current research interests include privacy and confidentiality, data masking, data and information security, and e-commerce.

Heng Xu is Assistant Professor and the founding director of the Privacy Assurance Lab (PAL) in College of Information Sciences and Technology (IST) at The Pennsylvania State University (Penn State). Her current research focus is on the interplay between social and technological issues associated with information privacy and security. Her research projects have been dealing with impacts of novel technologies on individuals' privacy perceptions, usable privacy and security, and design of privacy-enhancing technologies. Her Ph.D. dissertation on *Privacy Considerations in the Location Based Services* was a runner up for the 2006 ACM SIGMIS Doctoral Dissertation Award Competition. Her work has been published or accepted for publication in the *Journal of Management Information Systems, Information & Management, DATA BASE for Advances in Information Systems, Electronic Commerce Research and Applications,* and *Electronic Markets.*