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.