Decision Support Systems 54 (2012) 471–481

Contents lists available at SciVerse ScienceDirect

Decision Support Systems

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

Theories in online information privacy research: A critical review and an integrated framework

Yuan Li *

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

ARTICLE INFO

Article history:
Received 7 July 2011
Received in revised form 20 March 2012
Accepted 23 June 2012
Available online 2 July 2012

Keywords:
Online information privacy
Privacy concern
Privacy calculus
Risk calculus
Dual-calculus model

ABSTRACT

To study the formation of online consumers' information privacy concern and its effect, scholars from different perspectives applied multiple theories in research. To date, there has yet to be a systematic review and integration of the theories in literature. To fill the gap, this study reviews fifteen established theories in online information privacy research and recognizes the primary contributions and connections of the theories. Based on the review, an integrated framework is developed for further research. The framework highlights two interrelated trade-offs that influence an individual's information disclosure behavior: the *privacy calculus* (i.e., the trade-off between expected benefits and privacy risks) and the *risk calculus* (i.e., the trade-off between privacy risks and efficacy of coping mechanisms). These two trade-offs are together called the *dual-calculus model*. A decision table based on the dual-calculus model is provided to predict an individual's intention to disclose personal information online. Implications of the study for further research and practice are discussed.

1. Introduction

Much research has been conducted from various theoretical perspectives on individuals' concerns for information privacy in the e-commerce environment [14,49,59,74]. Such concerns reflect online consumers' worries that their personal information could be inappropriately collected, maintained, accessed, or used by online merchants without their consent [54,73,76]. Consumers who are concerned about online information privacy would take protective actions to reduce the risks, such as refusing to provide information to a website, providing inaccurate information, or removing information from a website [75]. These actions have significant impacts on online merchants that rely on customer information to provide personalized products and services [9,70,85].

To study online information privacy behavior, scholars from different perspectives adopted multiple theories in research, including the procedural fairness theory [20,83], the theory of reasoned action [24,64], the expectancy theory [24,35], the social contract theory [31,54], the protection motivation theory [17,88], and the social presence theory [60,89], among others. These theories interpret the formation of online consumers' privacy concerns and the subsequent behavior to provide (or conceal) personal information in online transactions. Based on these theories, a large number of antecedent and consequence factors of privacy concern were studied in literature [49,74].

In spite of the broad applications of theories in online information privacy research, there has yet to be a study to review the theories and to provide an improved understanding of the theoretical basis of the area. This leaves a number of limitations in literature. First, while the same kind of phenomena, i.e., the privacy-driven behavior, was investigated through multiple theories, the theories address the issue from different perspectives with varied emphases: some focus on organizational factors that influence an individual's privacy perceptions, such as the procedural fairness theory and the social presence theory [20,60,89], while others focus on individuals' internal responses to the external factors, such as the protection motivation theory [17,88]. Such distinct emphases in theories suggest that applications of multiple theories in a study may help to produce more fruitful results in understanding the phenomena, calling for a theoretical review, comparison, and integration [69].

Second, while the theories address privacy issues from different perspectives, there are connections among the theories that need to be recognized. For example, the privacy calculus theory is a common approach to analyzing individuals' information disclose behavior, suggesting that an individual's intention to disclose information is based on the comparison of expected benefits and perceived risks in a given context [20,22,24,83]. Although the specific benefit and risk factors differ across studies, depending on other theories applied, the general findings support the central role of the privacy calculus [74]. Recognizing such a connection between theories is helpful in fortifying the theoretical basis of this area, which is critical for studies that draw upon multiple theories.

Third, facets of theories that have not received full attention in literature should be recognized and strengthened in further research.

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

0167-9236/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.dss.2012.06.010

Scholars operationalize certain aspects of the theories to fit their research objectives. For example, the theory of reasoned action (TRA) [4] suggests that a person's behavioral intention is influenced by two antecedent factors: attitude and subjective norm. The privacy literature adopting this theory has analyzed either attitude [8,37,71] or subjective norm [21] but not both, and some examined none of them [24,41,42,53,54]. By recognizing the under-investigated areas of theories in literature, it is possible to conduct research for improved outcomes.

To address the above limitations, this study reviews fifteen established theories in online information privacy research and develops an integrated theoretical framework for future research. The study has three potential contributions. First, it provides a comprehensive view of the theoretical basis of this area. Although several review studies were conducted in this area [14,49,59,74], none has focused on the underlying theories in research. The current study therefore fills the gap in literature. Second, the integrated framework provides a basis for further research by summarizing achievements made in this area and highlighting new research opportunities, as discussed in Section 5. Third, a new trade-off in information disclosure decisions – the *risk calculus* – is derived from the protection motivation theory [66], which refers to the trade-off between perceived risks and the efficacy of coping with the risks. The risk calculus and the well-known privacy calculus [74] constitute the *dual-calculus model*, which determines the intentions of individuals to disclose information online. This model has potential values for research and practice.

The rest of the article is organized as follows. Section 2 describes the research method. Section 3 presents the review. The integrated framework is proposed in Section 4, where the relationships among the theories are explained. Finally in Section 5, limitations of the study and implications for research and practice are discussed.

2. Research method

This study follows the common approach of literature review [47,69]. Based on the research objectives specified above, the first step is to select and filter theories from the literature. While many theories and frameworks were applied to study online information privacy, it goes beyond the scope of this study to review them all. Instead, the study focuses on established theories that have been empirically tested at the individual level. First, only established theories are selected, and references (such as research models and frameworks) that did not reach the status of a theory [78] are excluded. Here a theory refers to the statement of the relationship between variables or constructs [10], and established theories are those that contain specific sets of variables or constructs in certain relationships that are consistently studied across literature. A key indicator of such a theory is its commonly cited name, such as TRA [4]. This criterion ensures that the review recognizes a robust theoretical basis of this area.

Second, only theories that have been studied at the individual level are selected. While prior studies show that privacy concern is a multilevel construct ranging from individual concern to societal concern [14,74], the majority of the information privacy literature is based on the individual level [59]. Although the other levels of privacy concern have potential impacts on individual concern, the development of a cross-level theoretical framework is beyond the scope of the study. Therefore, privacy-related theories that are not at the individual level, such as the institutional theory and the resource-based view [34], are excluded.

Finally, the study includes theories that have been empirically tested in online information privacy literature in order to develop a framework with empirical evidences. Theories that were not empirically tested in privacy literature are excluded. These three criteria are used to select articles from literature; potential limitations of these criteria are discussed in Section 5.1.

The search process focuses on articles published since 1996 when Smith et al. [73] developed a popular scale to measure information privacy concerns. Via a search in online research databases including *EBSCO* and *ScienceDirect*, over eighty empirical studies were recognized, based on which fifteen established theories were selected. Table 1 lists the theories with brief descriptions and exemplary articles. The review of the theories, along with definitions of key constructs, is presented in the next section.

3. Review of the theories

The fifteen theories interpret online information privacy from different but interrelated perspectives. Fig. 1 provides a map for the review, which categorizes the theories based on the origin, the behavioral consequences, and the influential factors of privacy concern. Two theories that explain the origin of privacy concern are introduced first; they are the agency theory [16,30] and the social contract theory [28,55]. Both suggest that uncertainties, such as privacy concerns, exist in online transactions due to incomplete information of online merchants' opportunistic behavior regarding customer information. Because of the privacy concerns, customers are hesitant to disclose information online. The relationship between privacy concern and information disclosure is further specified in the theory of reasoned action (TRA) [4] and the theory of planned behavior (TPB) [1].

Privacy concern is not the only factor that influences information disclosure; other factors, such as perceived benefits, also have an impact. To study the joint effect (or trade-off) of the opposing factors on the behavior, the privacy calculus theory [46] is discussed, including three various forms: the utility maximization theory [9], the expectancy theory of motivation [77,80], and the expectancy-value theory [1,2]. These theories are introduced in sequence.

Finally, theories that study the influential factors of privacy concern are reviewed. These include theories that explain the institutional factors (including the procedural fairness theory [20,52,77], the social presence theory [65,72], and the social response theory [57,81]) and theories that explain the individual factors (including the protection motivation theory [32,66], the information boundary theory [6,62], the social cognitive theory [11,12], and the personality theories).

3.1. Agency theory

The agency theory, as shown in Table 1, outlines the transactional relationship (called *agency relationship*) between a principal and an agent, who are both self-interested parties [16,30]. It suggests that as information regarding the behavior of the agent is often incomplete and asymmetric, the principal is unable to fully monitor the agent's behavior before and after the transactions, which gives the agent the opportunity to serve self-interests instead of those of the principal. To reduce the cost caused by opportunistic behaviors of the agent, the principal needs to incur additional monitoring cost. The sum of opportunity cost and monitoring cost is known as *agency cost*, and the theory proposes economic and social mechanisms to reduce agency cost, such as making effective contracts [16,30].

In online transactions, as the consumer (i.e., the principal) provides personal information to the merchant (i.e., the agent) for goods and service, the agency relationship is in effect. As both are self-interested parties and information asymmetry favors the online merchant who collects and uses customer information during and after the transactions, uncertainties such as privacy risks exist regarding the information use. Therefore, the consumer needs to decide whether to provide information to participate in the transactions and if so, how the potential risks can be mitigated. On the other hand, laws and regulations (such as the *Fair Information Practice* or FIP) help to transfer some of the