Electronic Commerce Research and Applications 13 (2014) 32–44

Contents lists available at ScienceDirect

Electronic Commerce Research and Applications

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

A multi-level model of individual information privacy beliefs

Yuan Li *

Division of Business, Mathematics and Sciences, Columbia College, Columbia, SC 29203, United States

ARTICLE INFO

Article history:
Received 26 September 2012
Received in revised form 11 August 2013
Accepted 11 August 2013
Available online 22 August 2013

Keywords:
Behavioral impacts
E-commerce
Information disclosure
Information privacy
Multi-level model
Online behavior
Psychological needs
Risk
Privacy beliefs

ABSTRACT

Several types of individual information privacy beliefs have been studied in literature, but their distinctions, relationships, and behavioral impacts have yet been systematically analyzed, causing difficulties in comparing and consolidating results across literature. Based on a review on various types of privacy beliefs, this study develops a multi-level model to strengthen this concept. The model consists of three levels of privacy beliefs, including: disposition to privacy, representing a person's fundamental beliefs and overall propensity to value privacy across contexts; online privacy concern, representing a person's overall perception of privacy risks in the online environment; and website privacy concern, representing a person's perception of privacy risks on a particular website. An empirical test reveals that disposition to privacy has a positive impact on both online privacy concern and website privacy concern, and website privacy concern is the only significant predictor of intentions to disclose information and transact on a website. The study helps to synthesize individual information privacy beliefs and assists in understanding their impacts on online behavior.

1. Introduction

In the e-commerce environment, individuals' information privacy beliefs, such as their privacy concerns, play important roles in determining their online behavior (Hoadley et al. 2010, Kauffman et al. 2011). Various studies have been conducted to measure privacy beliefs (Buchanan et al. 2007, Dinev and Hart 2004, Malhotra et al. 2004, Stewart and Segars 2002) and to examine the antecedents and consequences (Belanger and Crossler 2011, Li 2011, Pavlou 2011, Smith et al. 2011). In general, there is strong evidence to suggest that a person's privacy beliefs affect a number of psychological and behavioral consequences such as online trust and intentions to disclose information online (Li 2011, Smith et al. 2011). Awareness of consumer privacy concerns drives online firms to develop privacy policies to deal with the concerns (Cranor et al. 2008). A good example is the change of the privacy policy by Facebook.com (e.g., adding opt-out and access limit) in dealing with a public outcry against their information practice (Hoadley et al. 2010).

To date, a number of individual information privacy beliefs have been studied in literature. One is Internet privacy concern or general privacy concern (Li et al. 2010, Li 2011, Liao et al. 2011), which measures a person's overall perception of privacy risks on the Internet. A second is specific privacy concern or situation-specific concern (Li et al. 2010, Li 2011, Liao et al. 2011), which deals with a person's perceptions of privacy risks in a specific situation or on a particular website. And a third is disposition to privacy or psychological need for privacy (Rensel et al. 2006, Xu et al. 2011, Yao et al. 2007), which addresses a person's fundamental beliefs about privacy needs. Meanwhile, other types of privacy beliefs were also analyzed, such as privacy anxiety and perceived importance of privacy (Chai et al. 2009, Hossain and Prybutok 2008). These types of privacy beliefs demonstrate the multi-faceted nature of the concept in the online environment.

Except for a few studies that recognized the preliminary difference between the privacy beliefs (Faja and Trimi 2006, Li et al. 2010, Li 2011, Liao et al. 2011), there has yet to be a systematic investigation of these beliefs. This has caused difficulties for comparing and consolidating the results across the literature. For example, studying the impact of privacy beliefs on trust, Chiu et al. (2009) found that perceived privacy has a positive impact on consumer trust in an online vendor, but Bansal et al. (2010) did not find support for this effect in a healthcare website. The distinction resides in the types of privacy beliefs measured: Chiu et al. measured privacy beliefs with regard to the specific online vendor while Bansal et al. measured the general concern about health information privacy on the Internet. In another example, Kauffman et al. (2011) compared two studies by Hui et al. (2007) and Pavlou et al. (2007) on the impact of privacy concerns on consumer behavior. They suggested that the two draw distinct conclusions. Hui et al. measured consumer privacy concern with

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

1567-4223/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.elerap.2013.08.002

regard to the Internet while Pavlou et al. measured it with regard to specific websites. These examples highlight the need to distinguish between the various types of privacy beliefs and to examine their distinct impacts on consumer behavior in order to apply this concept more precisely in further research.

This study attempts to answer three research questions. (1) What are the different types of individual information privacy beliefs studied in literature? (2) How are they related? (3) What are their impacts on an individual's intentions to disclose information and transact on a website? Inspired by the e-commerce literature on trust beliefs (McKnight and Chervany 2002, McKnight et al. 2002), I develop a multi-level model to clarify the privacy belief concept, including disposition to privacy, online privacy concern, and website privacy concern. *Disposition to privacy* represents a person's overall propensity to value privacy across contexts. *Online privacy concern* represents a person's overall perception of privacy risks in the online environment. *Website privacy concern* stands for a person's perception of privacy risks on a specific website. I also analyze the relationships between the privacy beliefs and their impacts on behavioral intention. Finally, I empirically test the model representing a set of related relationships.

I offer two potential contributions to the online privacy literature. First, I strengthen the conceptualization of individual information privacy beliefs, highlighting the distinctions among the beliefs and their relationships. This provides a basis to consistently interpret the concept across literature and to incorporate other possible levels of privacy beliefs that may have been overlooked. Second, I present a systematic view on the impacts of privacy beliefs on individual online behavior, enabling researchers to specify this concept more precisely in further research.

2. Literature

I begin with a review on studies on individual information privacy beliefs to better understand this concept. While different terms such as privacy beliefs, attitudes, and concerns have been used to describe the concept (Smith et al. 2011), they all measure a person's privacy perceptions and are sometimes used interchangeably (Kauffman et al. 2011). Therefore, I use the term *privacy beliefs* to refer to this category of concepts and use more specific terms such as *privacy concern* wherever necessary. In addition to the three aforementioned privacy beliefs (Internet or general privacy concern, situational or specific privacy concern, and disposition to privacy), other types of privacy beliefs were also analyzed in literature, such as information privacy anxiety (Chai et al. 2009), perceived privacy control (Connolly and Bannister 2007), perceived importance of personal privacy (Hossain and Prybutok 2008), privacy protection belief, and privacy risk belief (Li et al. 2010). These constructs have been studied less frequently, so that I focus on the three major types of privacy beliefs in this study. As these constructs can be better understood via their nomological networks with other antecedents and consequences, I summarize these beliefs in Table 1.

2.1. Privacy beliefs regarding the Internet

This type of privacy beliefs, sometimes referred to as Internet privacy concern (Dinev and Hart 2004, Malhotra et al. 2004) or general privacy concern (Li et al. 2010, Li 2011, Liao et al. 2011), measures a person's overall perception of privacy risks on the Internet. It is widely studied as a multidimensional construct capturing a person's concerns about the finding, abuse, collection, and control of personal information on the Internet (Dinev and Hart 2004, Malhotra et al. 2004). Although unidimensional scales are also used to measure the construct (Dinev and Hart 2006, Liao et al. 2011), they are primarily adopted from the existing multidimensional scales, especially the four-dimensional scale of concerns for information privacy (CFIP) (Smith et al. 1996, Stewart and Segars 2002).

Prior studies have shown a number of antecedents to a person's privacy concern about the Internet, including personal experience with the Internet and cultural background (Bellman et al. 2004); perceived vulnerability on the Internet (Dinev and Hart 2004); a person's Internet literacy, risk perception, and social awareness (Dinev and Hart 2005, 2006; Liao et al. 2011); and personality traits such as agreeableness, conscientiousness, and openness to failure (Junglas et al. 2008). These factors reflect a person's overall values, knowledge, and experience regarding online privacy and are not restricted to specific websites or online situations.

The psychological and behavioral consequences of Internet privacy concern also have been examined. For psychological consequences, Awad and Krishnan (2006) have shown that privacy concern about e-commerce websites enhances the perceived importance of information transparency in online transactions; Malhotra et al. (2004) reported that Internet users' information privacy concern (IUIPC) reduces trust beliefs and enhances risk beliefs in online firms; and Kumar et al. (2008) have shown that CFIP influences the perceived usefulness of software firewall. For behavioral consequences, Son and Kim (2008) found that CFIP determines a number of privacy-protective responses such as refusal to provide information online and negative word-of-mouth, and Zimmer et al. (2010) reported that perceived privacy concern has a negative impact on information disclosure to a medical website. The impacts of Internet privacy concern on intentions to use the Internet for information disclosure and transaction have also been studied in literature (Dinev and Hart 2005, 2006; Liao et al. 2011).

Although the impact of Internet privacy concern on related psychological and behavioral consequences are observed in most literature, there are exceptions. For example, Hui et al. (2007) found that Internet privacy concern has no significant impact on information disclosure on a website, and Van Slyke et al. (2006) found that general concern for privacy has an impact on risk perception on a well-known websites (Amazon.com) but not on a less well-known websites (Half.com). Its impacts on trust and willingness to transact have been rejected for both contexts. The results may be interpreted in terms of the types of privacy beliefs measured: both studies measured privacy beliefs as general concerns for privacy on the Internet, although the behavioral consequences were for specific websites. So the direct relationship between the two is questionable.

2.2. Privacy beliefs regarding specific websites

This type of privacy beliefs, known as situation-specific privacy concern or specific concern (Li et al. 2010, Li 2011, Liao et al. 2011), measures individual privacy perceptions regarding specific websites or situations. Interestingly, this category of studies, as Table 1 shows, measures the specific privacy concern as a unidimensional construct, although many of the measurement items are adopted from the Internet privacy concern measures and especially the CFIP scale. In other words, information collection, use, and accuracy are typical items of the construct (Liu et al. 2005, Pavlou et al. 2007).

Similar to Internet privacy concern, this group of studies recognized a number of antecedents to situation-specific privacy concern. For example, Eastlick et al. (2006) has shown that the reputation of an e-tailer influences individual privacy concern about the e-tailer, and privacy concern influences trust in the e-tailer and intention to purchase from the e-tailer. Pavlou et al. (2007) found that pre-existing trust, website informativeness, and social presence of a website have direct impacts on privacy concern about the website, which then influences perceived uncertainty