International Journal of Information Management 43 (2018) 15–24

Contents lists available at ScienceDirect

International Journal of Information Management

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

An investigation of relationships among privacy concerns, affective responses, and coping behaviors in location-based services

Yoonhyuk Jung[a,*], Jonghwa Park[b]

[a] School of Business Administration, Ulsan National Institute of Science and Technology (UNIST), 50 Unist-gil, Ulsan, 44919, Republic of Korea
[b] Department of Management Engineering, Ulsan National Institute of Science and Technology (UNIST), 50 Unist-gil, Ulsan, 44919, Republic of Korea

ARTICLE INFO

Keywords:
Information privacy
Affect
Coping behavior
Location-based service
Laddering interview

ABSTRACT

Although information privacy has been extensively investigated in the information systems discipline, research heavily focuses on cognitive frameworks and underestimates the influence of affect on users' privacy behaviors. Psychological literature demonstrates that affect plays a significant role in individuals' decisions in risky situations. This study aims to explore associations between cognitive factors, affective responses, and coping behaviors in the context of privacy threats. For this purpose, we conducted a laddering interview with 56 users of location-based services. Elements elicited by an emerging coding procedure were mapped by their causal relations as described in interviews. The results revealed idiosyncratic associations among privacy concerns, affects, and coping behaviors, which implies that privacy concerns can result in different coping behaviors according to the affects following the concern. Thus, the result suggests that cognition-affect appraisals can offer a reliable framework for explaining users' privacy behaviors. This study proposes a new direction for the cognition-affect perspective in information privacy research by providing an alternative approach that reflects both cognition and affects to explain coping behaviors.

1. Introduction

Information privacy has been an important research topic within information systems (IS) over the last two decades. Information privacy threats have become more significant in the digital age because digitized personal information can be easily stored, duplicated, conveyed, and integrated in online environments (Junglas, Johnson, & Spitzmüller, 2008). Prior studies have demonstrated that information technology (IT) users place significant value on their information privacy (Chen, 2013), and the perception of information privacy risk is a major inhibitor of the adoption of IT services such as e-commerce (Dinev & Hart, 2006), mobile banking (Kim, Shin, & Lee, 2009), social networking services (Livingstone, 2008), and location-based services (Xu, Teo, Tan, & Agarwal, 2010). In particular, as big data techniques become increasingly prevalent, personal information including health, location, and online activity can be exploited for profiling, discrimination, and exclusion (Tene & Polonetsky, 2012). In addition, the emerging hyper-connected environments driven by Internet of Things (IoT) technologies have enabled the collection of personal information anywhere and at any time, even without individuals' awareness or consent, which can pose far graver threats to information privacy (Atzori, Iera, & Morabito, 2010). These emerging environments driven by big data and Internet of Things (IoT) technologies make information privacy even more critical.

Prior studies have developed diverse research models for understanding users' privacy behaviors, including *Concern for Information Privacy* (Smith, Milberg, & Burke, 1996), *Internet Users' Information Privacy Concerns* (Malhotra, Kim, & Agarwal, 2014), and *Information Privacy-Protective Responses* (Son & Kim, 2008). These models have improved our understanding of privacy behaviors by employing a multidimensional concept of privacy concerns and various types of coping behaviors. However, prior research that includes these research models is skewed toward cognitive-dominant frameworks and overlooks the role of affective factors in explaining users' privacy behaviors (Anderson & Agarwal, 2011; Li, Sarathy, & Xu, 2011). IS researchers have pointed out that cognitive frameworks have limitations in their capacity to explicate individual users' adoption of IT (Beaudry & Pinsonneault, 2010; Zhang, 2013). Affect is a fundamental human aspect that has a significant impact on people's decisions (Mittal & Ross, 1998) and influences their responses to risk or risk-related behavior (Loewenstein, Weber, Hsee, & Welch, 2001; Slovic et al., 1991). In particular, affects significantly influence behavioral responses by mediating the cognitive evaluation of risk (Bechara, Damasio, Tranel, & Damasio, 1997; Damasio, 1994). Cognitive reactions to environments

* Corresponding author.
E-mail addresses: yjung@unist.ac.kr (Y. Jung), bjh0515@unist.ac.kr (J. Park).

https://doi.org/10.1016/j.ijinfomgt.2018.05.007
Received 9 May 2017; Received in revised form 25 May 2018; Accepted 25 May 2018

(e.g., the perception of privacy risk) are used as inputs for humans' emotional processes, which subsequently influence their behavior (Bechara et al., 1997). Nevertheless, most IS studies on information privacy regard cognitive factors (e.g., privacy concerns) as the principal antecedents to users' intentions and behavior, and rarely examine the influence of affective factors (Anderson & Agarwal, 2011; Li et al., 2011).

This study explores the role of affective factors in the context of threats to information privacy with the goal of filling a void in the existing research on information privacy. More specifically, this study investigates the relationships between a particular type of privacy concern (e.g., unauthorized secondary use of personal information), a particular type of affect, and specific coping behavior. There are several sub-dimensions of privacy concerns, which may lead to different types of affect and coping behavior in response to information privacy threats. Privacy concern, which is a representative cognitive factor used in prior research on information privacy, is regarded as a multi-dimensional concept (Smith et al., 1996). Users may derive diverse types of negative emotions from using IT (e.g., anger, anxiety, disappointment) (Beaudry & Pinsonneault, 2010) and can choose different coping behaviors (e.g., refusal, negative word-of-mouth, complaint) to response (Son & Kim, 2008). The discovery of relationships among different types of privacy concerns, affects, and coping behaviors can offer rich and detailed explanations of users' privacy behaviors and ultimately improve our understanding of information privacy. Despite the potential merits, previous studies on information privacy have paid little attention to the associations among diverse types of privacy concerns, affects, and coping behaviors (Son & Kim, 2008). Accordingly, the objective of this study is to explore *how a particular type of information privacy concern leads to a particular type of affect which is subsequently associated with a specific coping behavior*.

This study employs a laddering interview approach to trace the detailed relationships from privacy concerns to affective responses to coping behaviors. This approach is used to extract individuals' hierarchically organized knowledge (Peffers, Gengler, & Tuunanen, 2003) and is employed as a way to discover individuals' reasoning behind their choices and preferences in information systems research (e.g., Peffers & Tuunanen, 2005; Tuunanen & Kuo, 2015). The study investigates the cognitive-affective appraisals of information privacy in the context of location-based services (LBS), which refers to a personalized service that identifies and transmits users' location information through their mobile devices (Junglas et al., 2008), such as online maps, location-specific mobile coupons, and augmented-reality games (e.g., Pokémon Go). While LBSs provide a more personalized service for users in combination with other information through users' spatial and temporal patterns, they may arouse privacy concerns for users through their collection, retention, usage, and disclosure of users' locations. Many researchers have thus investigated LBSs from a privacy perspective (Junglas et al., 2008; Xu et al., 2010). The current study contributes to information privacy research by examining the role of affective factors in explaining IT users' privacy behaviors and providing insight into the cognitive-affective processes users employ to cope with privacy risks.

2. Theoretical background

2.1. Concerns on information privacy and coping behaviors

Information privacy concerns (hereafter referred to as privacy concerns) refer to the extent to which individuals perceive a loss of control over their own personal information (Dinev & Hart, 2006). The understanding of privacy concerns is fundamental for the success of IT services (Hong & Thong, 2013), and privacy concerns are thus considered a central concept in IS research (Xu et al., 2010). There has been extensive research on diverse topics related to privacy concerns in the IS community, such as the development of privacy concern measurements (e.g., Malhotra et al., 2014; Smith et al., 1996), antecedents (e.g., Junglas et al., 2008; Xu et al., 2010) and outcomes (Jiang, Heng, & Choi, 2013; Son & Kim, 2008).

Even though the term 'concern' usually indicates a type of affect, 'privacy concern' has been widely used to refer to a perception of privacy invasion rather than an affective factor (Malhotra et al., 2014; Smith et al., 1996; Son & Kim, 2008). Furthermore, as an illustration of the exclusion of affective factors in information privacy research, Anderson and Agarwal (2011) explicitly regard privacy concern as a cognitive factor. Based on the privacy calculus perspective (Dinev & Hart, 2006), Anderson and Agarwal argue that privacy concern is a cognitive outcome of balancing the costs and benefits of privacy disclosure. Following their argument, we regard privacy concerns as a cognitive factor in this study.

Although some studies have dealt with privacy concerns as a unidimensional factor (e.g., Dinev & Hart, 2006), many other studies have employed a multidimensional concept of privacy concerns. Smith et al. (1996) conceptualized employees' perception of privacy risk as *Concern for Information Privacy* (CFIP), which is composed of four dimensions: collection, errors, unauthorized secondary use, and improper access. *Collection* indicates an individual's concerns about the extensive amount of their personal information that is collected and stored in databases; *errors* designates concerns about the accuracy of personal information's presentation; *unauthorized secondary use* represents concerns about the possible use of personal information for a purpose other than that for which it was collected; and *improper access* specifies concerns about personal information being readily available to unauthorized persons (Smith et al., 1996). Malhotra et al. (2014) developed another multifaceted construct, called *Internet Users' Information Privacy Concerns* (IUIPC), which consists of collection (which overlaps with CFIP), control, and awareness. *Control* indicates an individual's concerns about their limited control over IT service providers' use of personal information, and *awareness* is related to concerns about an individual's awareness of the information privacy practices of providers (Malhotra et al., 2014). These six factors from CFIP and IUIPC have been widely employed to examine and measure privacy concerns in the IS domain (Hong & Thong, 2013).

In terms of the consequences of privacy concerns, one critique is that research on information privacy concerns has mainly focused on a single type of response (e.g., refusal to provide personal information) (Son & Kim, 2008). Diverse reactions or coping behaviors are possible in response to information privacy threats. Coping refers to an individual's cognitive and behavioral efforts to manage stressful situations (Lazarus & Folkman, 1984). There are two types of coping behavior: problem-based coping and emotion-based coping. While the former constitutes direct behaviors employed to resolve a stressful situation, the latter involves indirect responses to a situation that deliberately change the meaning of a situation or control the emotions associated with it (Lazarus & Folkman, 1984). Despite frequent usage, this dyad classification of coping behaviors is criticized for its highly abstract conceptualization and the difficulty of determining whether a particular response corresponds to problem-based or emotion-based coping (Yi & Baumgartner, 2004). Therefore, diverse and specific types of coping behaviors such as planful problem solving, complaining, and behavioral disengagement are used to explain the behavioral consequences of stressful situations in behavioral research (Horwitz, Hill, & King, 2011; Mattila & Ro, 2008; Son & Kim, 2008; Yi & Baumgartner, 2004).

In addition to pointing out the limited examination of coping behaviors in IS studies on information privacy, Son and Kim (2008) suggested an examination of more diverse styles of user response to privacy risks. They proposed six specific types of information privacy-protective responses. Users who experience privacy threats from a service provider can refuse to provide personal information (*Refusal*) or intentionally provide falsified personal information (*Misrepresentation*). Users can also eliminate their personal information from the offending provider's