Government Information Quarterly xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

Government Information Quarterly

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

The role of privacy policy on consumers' perceived privacy

Younghoon Chang[a], Siew Fan Wong[b], Christian Fernando Libaque-Saenz[c], Hwansoo Lee[d,*]

[a] School of Management and Economics, Beijing Institute of Technology, China
[b] Department of Computing and Information Systems, Sunway University, Malaysia
[c] Department of Engineering, Universidad del Pacífico, Peru
[d] Department of Convergence Security, Dankook University, Republic of Korea

ARTICLE INFO

Keywords:
Privacy boundary management model
Privacy policy
Perceived privacy
Perceived effectiveness
Fair information practices
Trust
Privacy concerns

ABSTRACT

With today's big data and analytics capability, access to consumer data provides competitive advantage. Analysis of consumers' transactional data helps organizations to understand customer behaviors and preferences. However, prior to capitalizing on the data, organizations ought to have effective plans for addressing consumers' privacy concerns because violation of consumer privacy brings long-term reputational damage. This paper proposes and tests a Privacy Boundary Management Model, explaining how consumers formulate and manage their privacy boundary. It also analyzes the effect of the five dimensions of privacy policy (Fair Information Practices) on privacy boundary formation to assess how customers link these dimensions to the effectiveness of privacy policy. Survey data was collected from 363 customers who have used online banking websites for a minimum of six months. Partial Least Square results showed that the validated research model accounts for high variance in perceived privacy. Four elements of the Fair Information Practice Principles (access, notice, security, and enforcement) have significant impact on perceived effectiveness of privacy policy. Perceived effectiveness in turn significantly influences perceived privacy control and perceived privacy risk. Perceived privacy control significantly influences trust and perceived privacy. Perceived privacy concern and trust also significantly influence perceived privacy.

1. Introduction

We live in the era of big data that dramatically transforms the way we make decisions (Janssen, van der Voort, & Wahyudi, 2017). Big data is the "data sets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze" (Manyika, Chui, Brown et al., 2011). New information and communication technologies (ICTs) have enabled the big data trend by providing the capability to capture and store huge amounts of consumer data which serves as the core of the big data trend (Chen, Chiang, & Storey, 2012). When properly collected, stored, and processed, consumer data may allow organizations to understand customer behaviors and preferences. Such knowledge is valuable in customizing and personalizing products and services to meet customer needs, thereby equipping companies with a competitive advantage (Erevelles, Fukawa, & Swayne, 2016).

While businesses are eager to access customer data, privacy factor remains the most salient issue that must be solved before organizations could capitalize on the value of a data-centric service economy (Janssen & van den Hoven, 2015; TRUSTe, 2011). Given that each piece of data leaves behind electronic trails of customer activities, individuals are concerned about how companies collect and use their private information (Janssen & Kuk, 2016; Morey, Forbath, & Schoop, 2015) This situation, together with the increasing number of online information leaks, heightens customers' privacy concerns toward information risk (Drinkwater, 2016). Therefore, it is important that companies are aware and capable of handling the risks because they could pose long-term damaging effects on companies as well as cause economic losses (Culnan, 1993).

The risks have led governments to enact privacy regulations and policies (e.g., European Directive EC 95/461995 and United States Federal Trade Commission (FTC)'s Fair Information Practice Principles (FIPPs)) to protect people from potential harmful acts. Companies must comply with these regulations and devise effective privacy management strategies to address privacy issues. This would require knowledge of how people make decisions about revealing and concealing private information.

Petronio (2012)'s communication privacy management (CPM) theory used a boundary metaphor to explain how people make decisions about revealing and concealing information, which is known as 'privacy boundary formation.' In impersonal contexts such as those

* Corresponding author.
E-mail addresses: cf.libaques@up.edu.pe (C.F. Libaque-Saenz), hanslee992@gmail.com (H. Lee).

https://doi.org/10.1016/j.giq.2018.04.002
Received 28 June 2017; Received in revised form 23 April 2018; Accepted 23 April 2018

between customers and companies, the form by which companies use customer data (i.e., organizational information practices) is salient to the formation of an individual's privacy boundary (Dinev, Xu, Smith, & Hart, 2013; Metzger, 2007). In the process of forming privacy boundary, consumers also reference their governments' privacy regulations (Xu, Dinev, Smith, & Hart, 2011).

Weighing the interplay among consumers' privacy boundary formation, organizations' information practices, and government's regulations as well as the current findings in the literature, we realize that there are gaps that have to be addressed so that a better understanding of consumers' privacy boundary formation can be achieved. First, previous research has not fully examined the effect of government's privacy policy. In fact, these studies are either considering only some of the dimensions (e.g., Libaque-Saenz, Chang, Kim, Park, & Rho, 2016; Libaque-Saenz, Chang, Wong, & Lee, 2015; Libaque-Saenz, Wong, Chang, Ha, & Park, 2016) or have not even delved into its specific dimensions at all (e.g., Xu et al., 2011; Xu, Teo, Tan, & Agarwal, 2012). Since each principle of the privacy regulations may have different effect, organizations need to determine which is exerting stronger impact on individuals' decisions in order to draw adequate strategies (Schwaig, Kane, & Storey, 2006),

Second, while prior research has focused on various dependent variables such as privacy concerns, intrinsic motivation, trust, information sensitivity, intention to disclose personal information and compliance intention (e.g., Bansal, Zahedi, & Gefen, 2010; Dinev & Hart, 2006a; Joinson, Reips, Buchanan, & Schofield, 2010; Lee, Lim, Kim, Zo, & Ciganek, 2015; Lowry, Cao, & Everard, 2011; Tsai, Egelman, Cranor, & Acquisti, 2011), it has not placed the complete organizational information practices within the recursive and wholeness view of privacy boundary formation model to explore their effect in the online context. Recognizing this gap, researchers (e.g., Bansal & Gefen, 2015; Dinev et al., 2013; Kehr, Kowatsch, Wentzel, & Fleisch, 2015) have called for scholars to further explore online privacy boundary formation and rationality.

Our research aims to fill these two research gaps by proposing and empirically testing a Privacy Boundary Management Model (PBMM) that is grounded on Petronio (2012)'s Communication Privacy Management Theory, Higgins (1997)'s Regulatory Focus Theory and Xu et al. (2011)'s application of CPM in the context of information privacy to provide a complete view of customers' privacy boundary management process. We collected the data from bank customers in Malaysia who are using online banking services because the banking sector contains a wealth of sensitive private information that many consumers would be reluctant to disclose to third parties. Therefore, we expect these consumers to act more conservatively as regards the sharing and disclosure of their banking data.

The rest of the paper is structured as follows. Section 2 reviews the theoretical background and section 3 discusses the research model and the hypotheses. Section 4 describes the research method while section 5 discusses the results. Section 6 provides the discussion, implications, research limitations, future research, and concluding remarks.

2. Theoretical background

2.1. Online banking

Online banking refers to the use of banking services through the Internet (Yiu, Grant, & Edgar, 2007). Although it started as a channel to present information, this technology has evolved and nowadays allows customers to perform various transactions such as paying bills, transferring money, and checking account balances through the bank's website. The use of this technology has expanded worldwide due to its cost savings and convenience (Pikkarainen, Pikkarainen, Karjaluoto, & Pahnila, 2004). As a result, banks have enlarged their customer databases and they could benefit from the analysis of these data to launch personalized marketing campaigns and innovative services in order to maintain a competitive advantage.

However, there are also challenges in using customer data in the online banking context. Apart from technical challenges such as the techniques and technology requirements to handle this massive amount of data (Sun, Morris, Xu, Zhu, & Xie, 2014), privacy concerns may also represent a barrier. In the context of online banking, individuals and banks interact by exchanging not only monetary resources but also information such as the identity of the user, bank account status, transfers, and payments. These sensitive information may raise individuals' concerns about potential threats. Whereas, the occurrence of any online information leak may represent serious problems to banks because as a highly regulated market as it is, banks must comply with current regulation on personal data protection. Accordingly, individuals' assessment on how banks handle their information becomes important in this domain.

2.2. Communication privacy management theory

Petronio (2002)'s Communication Privacy Management Theory (CPM) is a communication theory that encompasses the way in which confidants handle disclosed information. CPM argues that individuals have a dynamic boundary to maintain their privacy, and they manage the boundary by their own rules (Baruh, Secinti, & Cemalcilar, 2017; Sutanto, Palme, Tan, & Phang, 2013). In the context of online banking, individuals and banks interact by exchanging not only monetary resources but also information such as the identity of the user, bank account status, transfers, and payments. This sensitive information may raise individuals' concerns about potential threats. Accordingly, individuals' assessment on how banks handle their information becomes important in this domain. Hence, CPM is appropriate for our research.

CPM uses a boundary metaphor to explain how people as data owners make decisions about revealing and concealing private information (Petronio, 2012). An individual's privacy boundary encompasses information that only he/she has, but others do not know. This privacy boundary is built on people's belief that they own their private information and therefore want to maintain control of what, when, and with whom it is shared. Information within a personal boundary is considered private and is not disclosed to others. When private information is accessible to only one individual, the boundary is considered thick because there is less possibility for the information to be leaked to the public. Once private information is shared with another party, the boundary becomes thin and permeable, which increases the possibility of information becoming public.

Accordingly, CPM posits five core principles: 1) people believe they own and have a right to control their private information; 2) people control this information through the use of personal privacy rules; 3) when others are given access to a person's private information, they become co-owners of that information; 4) co-owners of private information need to negotiate mutually agreeable privacy rules; and 5) when co-owners of private information do not effectively negotiate and follow mutually held privacy rules, turbulence ensues (Petronio, 2002).

The first principle is consistent with Westin's (1967) definition of information privacy as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.” According to this principle, when individuals decide to disclose personal information, they assess the level of privacy they have at the time the assessment is made (Xu et al., 2011).

The second principle highlights CPM as a rule-based theory. Under this rule-based approach, CPM attempts to focus on the factors driving individuals' privacy boundary decisions. CPM posits that those factors are cost/benefit ratios, context, culture, motivation, and gender. As theorized by Xu et al. (2011), risk and control represent two important concepts that individuals assess to balance the costs and benefits involved in privacy disclosure. Depending on the assessment outcome, individuals determine how much control they have toward the