International Journal of Information Management 36 (2016) 531–542

Contents lists available at ScienceDirect

International Journal of Information Management

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

Intention to disclose personal information via mobile applications: A privacy calculus perspective

Tien Wang[a,*,1], Trong Danh Duong[a,1], Charlie C. Chen[c]

[a] Institute of International Management, College of Management, National Cheng Kung University, Tainan, Taiwan R.O.C. No.1, University Road, Tainan City 701, Taiwan, ROC

[c] Department of Computer Information Systems & Supply Chain Management, Appalachian State University, Boone, NC, USA, 287 Rivers St, Boone, NC 28608, USA

ARTICLE INFO

Article history:
Received 18 September 2015
Received in revised form 1 March 2016
Accepted 2 March 2016
Available online 14 March 2016

Keywords:
Privacy calculus
Intention to disclose
Privacy concerns
Information privacy
Mobile applications

ABSTRACT

This study aimed to investigate the issue of consumer intention to disclose personal information via mobile applications (apps). Drawing on the literature of privacy calculus theory, this research examined the factors that influence the trade-off decision of receiving perceived benefits and being penalized with perceived risks through the calculus lens. In particular, two paths of the direct effects on perceived benefits and risks that induce the ultimate intention to disclose personal information via mobile apps were proposed and empirically tested. The analysis showed that self-presentation and personalized services positively influence consumers' perceived benefits, which in turn positively affects the intention to disclose personal information. Perceived severity and perceived control serve as the direct antecedents of perceived risks that negatively affect the intention of consumers to disclose personal information. Compared with the perceived risks, the perceived benefits more strongly influence the intention to disclose personal information. This study extends the literature on privacy concerns to consumer intention to disclose personal information by theoretically developing and empirically testing four hypotheses in a research model. Results were validated in the mobile context, and implications and discussions were presented.

1. Introduction

The ownership of mobile devices and mobile media use have reached the tipping point of exceeding desktop ownership and wired media usage. The total number of mobile subscriptions worldwide is approximately 6.8 billion (International Telecommunication Union, 2013). As of 2013, 65% of U.S. mobile consumers had their own smartphones (Fingas, 2014), and in 2014, 519.7 million people in China were smartphone users, with the number estimated to increase to 700 million by 2018 (Millward, 2014). The rapidly increasing mobile subscriptions and the growing popularity of smartphones and tablet devices equipped with billions of applications (apps) have unleashed new marketing possibilities. As such, marketers incessantly develop innovative strategies for exploiting mobile devices (e.g., tablet, wearable smartwatch, and smartphone) to provide consumers with additional relevant mobile contents and services, such as personalization, socialization, and self-presentation opportunities.

However, the fundamental success of any creative mobile app or service depends on the acquisition of personal information from users. For instance, location-based services are not significantly beneficial to mobile users if they refuse to share with mobile service providers a certain level of information granularity about their whereabouts at a specific time. Most mobile users believe that releasing personal information has potential risks to the violation of their privacy. From users' standpoints, when they agree to offer personal information about what and how they do in daily lives with location and time data, they can better present themselves in a virtual world. For example, posting selfies on various social networking sites not only reveals personal interests but also leaves digital footprints, allowing marketers to analyze consumer profiles. The check-in function of Facebook also allows marketers to perform location-based marketing. The possession of hand-held devices with mobile technology allows consumers to access mobile applications, social media accounts, online games, and brand communities and to receive truly personalized services

* Corresponding author.
E-mail addresses: twang@mail.ncku.edu.tw (T. Wang), danhdt12a8@gmail.com (T.D. Duong), chench@appstate.edu (C.C. Chen).
[1] [1]Fax: +886 6 2751175.

http://dx.doi.org/10.1016/j.ijinfomgt.2016.03.003
0268-4012/

at the right location and right time. For mobile service providers, when they collect customers' information regarding who, what, how, where, and when they do certain things, the providers become closer to the physical aspects of customers' daily lives and perhaps to the psychological aspects of inner self. The richness of information exchanged in the mobile context is far more than those in a purely internet, desktop-based environment. Another facet of such personal information disclosure in the mobile context is that it presents both benefits and risks to users, whereas it only involves benefits to service providers. The process of enticing users into agreeing to share their personal information via their mobile devices has become a strategic business issue that should be primarily resolved before the mobile business (m-business) can deliver personalized products or services to customers.

In the m-business era, consumers are attracted to countless features and apps on mobile devices, such as social media, games, location-based services, real-time news, investment tools, entertainment, travel guides, traffic updates, music, and e-books. To maximize the features of mobile apps or receive promotional materials (e.g., emoticons, points, and coupons), consumers are often asked to share their postings, photos, location, payment, and other related personal information. The disclosure of the high granularity of personal information increases the risk of compromising or misusing personal information (Awad & Krishnan, 2006). The paradox of enjoying personalized services and taking the risk of losing personal information is evident in m-business. In the face of such paradox, the e-business needs to seek approaches for showing users that they would receive more benefits than the potential cost caused by information misuse of the vendor and its affiliated partners.

Information privacy has been extensively explored in both the physical (Goodwin, 1991) and digital worlds (Barwise & Strong, 2002; Chellappa & Sin, 2005; Sutanto, Palme, Tan, & Phang, 2013; Xu, Liao, & Li, 2008). Consumers are concerned about the inappropriate collection, storage, profiling, and use of their personal information for unintended purposes without their consent (Keith, Thompson, Hale, Lowry, & Greer, 2013). The privacy calculus model, which suggests that consumers engage in a risk–benefit analysis when they share information with the vendor, has been adopted in previous studies (Laufer & Wolfe, 1977; Xu, Luo, Carroll, & Rosson, 2011). Drawing on this theoretical model, the current study aims to propose and empirically test a research model on consumer intention to disclose personal information through mobile apps. Accounting for the simultaneity of the trade-off mental calculation in the mobile environment, the benefits and risks involved in personal information disclosure in this context are proposed and realized in a dual path model specification. The antecedents of both the perceived benefits and risks are simultaneously examined in the model to present a balanced view. Personalized service and self-presentation are particularly proposed as key forces that drive perceived benefits because the mobile technology enables marketers to better design their promotional offers to consumers at the individual level at a specific time and location once they have multifaceted personal data. The service level can be lifted to a highly sophisticated and delicate level beyond the one based on a purely internet-based approach. The possession of digital services and entities also reveals and portrays self-concepts more vividly. The importance of perceived severity and perceived control is further intensified in the mobile context. The mobile technology connects numerous elements into a thicker and broader web, creating a new world (i.e., The Internet of things, IoT). Such influence continuously occurs, gradually changing people's lives in a subtle but extensive manner. Once mobile users agree to disclose their personal information, they are led to a tight web of connected elements in which information exchange can go beyond their comprehension level.

With these research attempts, this study contributes to the literature in several ways. First, this research examines the role of psychological factors in privacy calculus theory and proposes an affective-based privacy calculus model to examine disclosure intention in the mobile context. Four psychological antecedents that influence users' perceptions of the benefits and risks associated with the revelation of personal data are proposed and empirically investigated to provide practicing managers with strategic insights. Through investigating the dual paths of influences resulting from the perceived benefits and risks in one model, this research also examines the differential effects of these dimensions that are not addressed in the existing literature on privacy calculus. The empirical findings suggest new research opportunities to further enhance our knowledge on privacy calculus and disclosure intention.

Second, the dual factors of the privacy calculus model, namely, benefits and risks, are investigated simultaneously to clarify whether the mental calculation on both paths works in tandem. Through this approach, this study provides a holistic view of the positive and negative forces that influence the intention of mobile app users to reveal personal information.

The remainder of this paper is organized into five sections. Following the Introduction, Section 2 explains the proposed research model based on the privacy calculus model and presents the research hypotheses. Section 3 describes the research methodology. Section 4 presents the empirical findings and model results. Finally, Section 5 provides the conclusion coupled with theoretical contributions, management implications, and limitations of this study, as well as suggestions for future research.

2. Conceptual foundation and research hypotheses

Absolute privacy can hardly be achieved in the digital world. The privacy calculus model (Laufer & Wolfe, 1977) is commonly used to analyze the privacy perceptions and behaviors of consumers. Privacy calculus is a function that shows how consumers decide whether to disclose their personal information based on the results of a calculation from disclosure needs and privacy concerns in a specific information-disclosure context (Xu, Teo, Tan, & Agarwal, 2009). Privacy calculus serves as a function of consumers' expectations of positive and negative outcomes before deciding on what and how much information they will disclose to others (Li, 2012). Previous literature has suggested several driving factors of the benefits and risks in various research contexts, including traditional transactions (Culnan & Armstrong, 1999), online transactions (Dinev & Hart, 2004), government surveillance (Dinev, Hart, & Mullen, 2008), and location-aware marketing (Xu et al., 2011).

This study adopts privacy calculus theory as the research basis and proposes that two paths can lead to the intention of personal information disclosure via mobile apps (Keith et al., 2013; Li, Sarathy & Xu, 2010; Xu et al., 2011; Xu et al., 2009). The first path reveals a positive effect from perceived benefits, whereas the second path presents a negative influence from perceived risks. The perceived benefits of information disclosure via mobile devices and applications appeal to different customers. For instance, customers engaged in m-banking can instantly receive information based on their latest transactions, and they can learn how each transaction could affect their monthly spending budget (Khasawneh, 2015). Travelers receive personalized ancillary services via their mobile phones to improve their travel experience (Morosan, 2015). Grocery buyers can expedite the check-out process and readily receive coupons via their mobile phones to save time and money (Danaher, Smith, Ranasinghe, & Danaher, 2015). In nursing homes, caregivers can receive recommended drugs via drug reference software installed in their mobile devices to avoid adverse drug events (Handler, Boyce, Ligons, Perera, Nace, & Hochheiser, 2013).