International Journal of Information Management 39 (2018) 49–59

Contents lists available at ScienceDirect

International Journal of Information Management

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

A bidirectional perspective of trust and risk in determining factors that influence mobile app installation

Amita Goyal Chin[a,*], Mark A. Harris[b], Robert Brookshire[c]

[a] Department of Information Systems, School of Business, Virginia Commonwealth University, Box 844000, Richmond, Virginia, 23284-4000, United States
[b] Augusta University Cyber Institute, School of Computer and Cyber Sciences, 1120 15th Street, University Hall/UH-127, Augusta, Georgia, 30912, United States
[c] University of South Carolina, Integrated Information Technology, College of Engineering and Computing, Columbia, SC, 29208, United States

ARTICLE INFO

Keywords:
Mobile device security
Mobile app installation
Institutionalized trust
Information security
Intent to install

ABSTRACT

The purpose of this research is to consider how trust in and perceived risk of a mobile marketplace impact a consumer before installing a mobile application. In particular, trust is considered from the perspective of institutionalized trust, where consumers faced with ignorance rely on institutionalized mechanisms for personal safety. A bidirectional research model is presented based on trust and perceived risk as antecedents to the intent to install a mobile application. Data is collected from a survey of 214 participants and is analyzed using structural equation modeling. Results suggest that institutional loyalty plays a significant role in consumers' intent to install mobile apps. Trust and its antecedent, security, had strong significant positive relationships with the intention to install mobile apps, while risk and its antecedent, privacy, had weak and insignificant relationships. The bidirectional model's relationship between trust and risk was also insignificant in both directions, further suggesting that perception of risk is an insignificant factor in the intent to install mobile apps.

1. Introduction

The smartphone market has reached 90 percent penetration in North America, Western Europe, Japan and parts of Asia/Pacific (Gartner, 3339019. And the demand for smartphones and tablets continues to increase. "Global sales of smartphones to end users totaled 373 million units in the third quarter of 2016, a 5.4 percent increase over the third quarter of 2015 (Gartner, 3516317). This ubiquitous infusion of smartphone and other mobile technology into the mainstream has radically altered workflow, personal activities, and our way of life, in general. Mobile technology, or mTechnology, includes phones, tablets, personal digital assistants (PDAs), gaming consoles, and e-readers (Harris & Patten, 2014) and has been so readily embraced that at over 7.22 billion, the number of mobile devices exceeds the number of people in the world, which is approximately 7.19 billion (Boren, 2014). mTechnology has alleviated the reliance on traditional desktop (and even laptop) computers in favor of the far more convenient portable handheld devices. mTechnology has become indispensable due to the plethora of widely and freely available mobile and 3G networks and the unprecedented and rapid proliferation of mobile applications. Mobile applications, or mApps, are programs that are specifically designed to run on mobile devices (Avinadav, Chernonog, & Perlman, 2015) and are available from several online venues including Apple, Google, Microsoft and BlackBerry app stores. Using these mApps, mTechnology is used for social interactions such as sending email, taking selfies and other photos, posting on social media, engaging in financial transactions, reading and researching online, among countless additional uses.

In juxtaposition to the burgeoning mApp market are concerns for consumer safety (Zonouz, Houmansadra, Berthiera, Borisova, & Sanders, 2013; Zhao, Zhang, Ge, & Yuan, 2012; van Cleeff, 2008; Wang, Streff, & Raman, 2012). As are desktop computers and laptops, mobile devices are susceptible to malware, privacy violations, and other infringements. However, data-centric security for mobile devices has largely been limited (van Cleeff, 2008), and no governmental regulations or other mandatory requirements have been instituted that compel users to proactively effectuate security measures (Jones & Chin, 2015). In fact, mTechnology safety and security has largely been neglected altogether (Gupta, Kumar, & Loothra, 2014).

Consumers are enlightened to at least the possibility of security infractions when downloading mobile applications. Therefore, trust becomes a key element of any mobile shopping, or mShopping, activity (Bisdikian et al., 2014). According to research and government agencies, some potential precautions that consumers can take are: review the mApp developers (IC3, 2012), use only trusted mApp markets, and evaluate the extensiveness of the mApp's permission requirements (Harris & Chin, 2016; Harris, Brookshire, & Chin, 2016). Prior to

* Corresponding author.
E-mail addresses: agchin@vcu.edu (A.G. Chin), marharris1@augusta.edu (M.A. Harris), brookshire@sc.edu (R. Brookshire).

https://doi.org/10.1016/j.ijinfomgt.2017.11.010
Received 29 May 2017; Received in revised form 16 November 2017; Accepted 29 November 2017
0268-4012/ Published by Elsevier Ltd.

installing an mApp, whether consciously or subconsciously, consumers undergo an evaluation process. This may take the form of assessing the risk of using mApps from particular developers (Harris, Patten, Brookshire, & Regan, 2015), checking the reputation of vendors (Harris & Chin, 2016), or reading reviews on particular online repositories (Harris, Chin, & Brookshire, 2015).

The purpose of this study is to assess how trust in and perceived risk of using mApp markets influence consumers' intention to install mobile applications on their mobile devices. In addition to considering trust as previously defined in research publications, this study includes the concept of institutional reliance as a component of consumer trust in situations of ignorance. Following a review of the extant literature relating to trust, institutional trust, and perceived risk, a research model is presented based on trust and perceived risk as antecedents to consumer intent to install a mobile application. A survey instrument is developed based on the multiple facets of trust as identified in previous works balanced with the assessment of risk and the perception thereof. Survey data is analyzed using structural equation modeling. Finally, we present our results and discuss the research implications of our findings.

2. Background

The portability, convenience, and explosive saturation of mTechnology combined with the massive proliferation of mApps that provide functionality for daily tasks and entertainment has enticed a voluminous and loyal following. While the frequent requirement of many of the mApps that run on mTechnology to disclose personal information has been disconcerting to consumers and may serve as somewhat of a deterrent for engagement in electronic commerce, or eCommerce (Dinev & Hart, 2006; Groß, 2016), online sales have continued to rise. Even though consumers are aware of the multifarious risks that accompany mShopping and realize that they cannot anticipate and mitigate all of these risks (Groß, 2016), they choose to participate in eCommerce, intrinsically assuming some level of institutional trust and subsequent personal protection. A calculus of a cumulative antecedent to information disclosure, where the consumer must balance multiple criteria including perceived risk, institutional norm, personal beliefs and trust, with anticipated benefit, to then settle on a paradoxical choice has been identified (Dinev & Hart, 2006; Culnan & Armstrong, 1999; Laufer & Wolfe, 1977). The pervasive literature abundantly encompasses studies focused on predicting human behavior, particularly in the context of a trust-risk relationship (Gu, Xu (Calvin), Xu, Zhang, & Ling, 2016; Hassoy, Durusoy, & Karababa, 2013; Hillman & Neustaedter, 2016; Qiu, Li, & Chen, 2013; Yan, Dong, Niemi, & Yu, 2013). In the present research, we draw from the technology acceptance model and expectation theory to understand user tendencies to install mobile applications in the context of known risk and institutional trust.

The technology acceptance model (TAM) by Davis (1989) attempts to understand user intentions with regard to the use and the acceptance of a technology. When presented with new technology, users are influenced by two major constructs: perceived usefulness (PU) and perceived ease of use (PEOU). PU is 'the degree to which a person believes that using a particular system would enhance his or her job performance' and PEOU is "the degree to which a person believes that using a particular system would be free of effort (Davis, 1989)." TAM is one of the most influential extensions of Ajzen and Fishbein's (1980) theory of reasoned action (TRA), which posits that behavioral intentions are the immediate antecedents to actual behavior and are influenced by beliefs about the likelihood that performing a particular behavior will lead to a specific outcome (Madden, Ellen, & Ajzen, 1992).

The classic expectancy theory of motivation developed by Vroom (1964) is often used to comprehend the process that individuals employ when choosing a decision amongst a multitude of behavioral options (Chiang, Jang, Canter, & Prince, 2008; Kiatkawsin & Han, 2017; Boundless, 2014; Renko, Kroeck, & Bullough, 2012). The expectancy theory states that individuals are motivated by the desire for an anticipated outcome. That is, in a causal relationship, individuals are likely to choose the effort that will lead to desirable rewards. Ghoddousi et al. (2013) constructed a model based on expectation theory to evaluate the motivation of construction workers and placed focus on intrinsic motivators to encourage these workers. Their study reaffirmed expectation theory in the context of the construction industry and recommended that workers should be satisfied intrinsically in order to garner high performance. Kiatkawsin & Han (2017) found that the facets of expectancy theory strongly influenced the pro-environmental behaviors of young group tour travelers. That is, when the travelers felt their actions and efforts would in fact contribute to the quality of the environment, this expectation positively influenced their intentions to behave sustainably. Purvis et al. (2015) applied expectancy theory to understand the extent to which stakeholders would participate in the implementation of project management systems and concluded that stakeholders assess the psychological climate surrounding a project and allow that expectation to determine their own actions of active support, token support, or counter-implementation actions.

Applying the TAM and expectation theories to mTechnology suggests that a consumer's decision to install an mApp will be influenced by the perceived usefulness of the mApp and by the perceived ease of use of the mTechnology in combination with their expectation of the personal benefits received from installing the mApp on the mTechnology. The indisputable popularity among all ages, races, and genders that has precipitated the omnipresence of mTechnology is a testament to its perceived usefulness and perceived efficacy of use. Given an a priori acclimation with their handheld device, the consumer's emphasis will then focus on the pursuit of the end reward – having the mApp available for use on their mobile device. The dominating desire for the resulting benefit – an increase in personal productivity or personal pleasure – then prevails over the notions of perceived risk in favor of an implicit assumption of institutional trust.

To understand user behavior to proceed with mApp installation even in the presence of perceived risk, we turn to Shepherd and Kay (2012) and their theory of motivated avoidance of sociopolitical information, which is based on system justification theory (Jost & Banaji, 1994) and the subsequent compensatory control theory (Kay, Gaucher, Napier, Callan, & Laurin, 2008). Shepherd and Kay (2012), invoking cognitive dissonance theory, argue that "to the extent that people increasingly trust or justify the legitimacy of an authority to cope with their dependence on it, they should be motivated to avoid information that could potentially rupture this trust" (Shepherd & Kay, 2012).

While the theory of motivated avoidance has never previously been applied to mShopping, and in particular, to the intent of consumers to install mApps, its theoretical propositions can be used to explain the psychological inclinations of complacency toward mApps security. The Shepherd and Kay (2012) model describes a behavioral path beginning with a "psychological discomfort associated with epistemic uncertainty." While the daily use of mTechnology has become comfortable and commonplace and its PU and PEOU incontrovertible, the technical aspects and the detailed web of actions that occur when engaging in mShopping, including downloading mApps, remains a source of perplexity and uncertainty for most individuals. This situation is further complicated with the readily available deluge of information and the multiplicity of mTechnology platforms. Securing one's mTechnology may be described as a complex activity, and the associated anxiety of the inability to decipher and process information particulars leads individuals to "simply outsource personal responsibility to supposed qualified others" (Shepherd & Kay, 2012).

Trust is a key underlying element of any transactional activity, where trust can be broadly defined as "the willingness of one party (trustor) to depend or rely on the actions of another party (trustee) (Bisdikian et al., 2014)." Users are unable to establish indisputable and absolute trust when mShopping but are unwilling to succumb to the fears of risk and uncertainty to the extent of disengaging from an online