International Journal of Information Management xxx (xxxx) xxxx

Contents lists available at ScienceDirect

International Journal of Information Management

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

Mobile application security: Role of perceived privacy as the predictor of security perceptions

Ali Balapour*, Hamid Reza Nikkhah, Rajiv Sabherwal

Department of Information Systems, Sam M. Walton College of Business, University of Arkansas, Fayetteville, AR, 72701, USA

ARTICLE INFO

Keywords:
Mobile applications
Communication privacy management (CPM)
Perceived privacy
Perceived security
Privacy policy

ABSTRACT

Despite mobile applications being at the frontier of mobile computation technologies, security issues pose a threat to their adoption and diffusion. Recent studies suggest that security violations could be mitigated through improved security behaviors and attitudes, not just through better technologies. Existing literature on behavioral security suggests that one of the main predictors of users' perceptions of security is their perceived privacy concerns. Using communication privacy management theory (CPM), this study examines the effects of privacy-related perceptions, such as privacy risk and the effectiveness of privacy policies, on the security perceptions of mobile app users. To empirically test the proposed theoretical model, two survey studies were conducted using mobile apps requesting less sensitive information (n = 487) and more sensitive information (n = 559). The findings show that the perceived privacy risk negatively influences the perceived security of the mobile apps; the perceived effectiveness of a privacy policy positively influences user perceptions of mobile app security; and perceived privacy awareness moderates the effect of perceived privacy risk on the perceived security of mobile apps. The results also suggest that users have different privacy-security perceptions based on the information sensitivity of the mobile apps. Theoretical and practical implications are discussed.

1. Introduction

Mobile apps have become an inherent part of everyday life. They have dominated individuals' digital habits due to the progress of mobile technologies, mobile access to high-speed internet, and the interactivity of mobile phone interfaces. From communicating to entertaining, mobile apps provide a variety of useful features that cause individuals to spend a great amount of time on their use (Reychav et al., 2019). A recent study demonstrated that individuals in the US spend an average of three and a half hours per day on mobile devices, with mobile apps comprising 90 % of internet time on smartphones and 77 % on tablets (Wurmser, 2018). As a result, a plethora of mobile apps are released into app marketplaces every day, to respond to demands for online shopping, games, finance management, and other tasks that users can complete with their mobile devices (Balapour, Reychav, Sabherwal, & Azuri, 2019; Balapour and Sabherwal, 2017). One report suggests that an average of 6140 mobile apps were released through the Google Play Store every day from the third quarter of 2016 to the first quarter of 2018 (Statista, 2018). However, despite these high numbers, most individuals in the US are hesitant to download mobile apps, with the number of downloads at an average of zero per month (Perez, 2017). Further research has shown that 80 % of users do not use the mobile apps they have downloaded after three months (Hopwood, 2017). Among the reasons why individuals do not install or continue to use mobile apps, users' concerns about security and privacy risks are found to be the most salient (Harris, Brookshire, & Chin, 2016; Levenson, 2016; Shah, Peikari, & Yasin, 2014) and merit further investigation.

The growth in the release and use of mobile apps is accompanied by the growth of mobile users' concerns about using them (Harris et al., 2016). Users are worried about the vulnerability of mobile apps, in terms of security, and that apps may possess malicious codes that track their activity, steal sensitive data, and make unauthorized calls (Kumar, 2016). Prior literature emphasizes that technical security methods alone are not enough to protect users, and there is a need to account for individual behavior in security studies (Posey, Roberts, Lowry, Bennett, & Courtney, 2013; Posey, Roberts, Lowry, & Hightower, 2014). Security concerns have been found to have a great impact on user intentions to install and continue using mobile apps (Harris et al., 2016). For example, Starbucks acknowledged in 2015 that hackers accessed customer accounts through the Starbucks mobile app, resulting in many mobile users removing this app from their devices due to security concerns (Gross, 2015; Pagliery, 2015). Users also have privacy concerns about using mobile apps and these concerns impact their perceptions (Shaw & Sergueeva, 2019). A report on mobile apps showed

* Corresponding author.
E-mail addresses: ABalapour@walton.uark.edu (A. Balapour), HNikkhah@walton.uark.edu (H.R. Nikkhah), RSabherwal@walton.uark.edu (R. Sabherwal).

https://doi.org/10.1016/j.ijinfomgt.2019.102063
Received 9 July 2019; Received in revised form 8 November 2019; Accepted 27 December 2019

that 52 % of users delete mobile apps and 40 % stop using apps because of privacy concerns (Mobile Ecosystem Forum, 2016). Mobile app developers need to better understand security and privacy perceptions, to decrease mobile users' concerns by devising appropriate security and privacy solutions, thereby attracting new users and retaining current ones. As security and privacy are the main concerns of mobile users for continuing to use apps, studying security and privacy perceptions and the relationship between them can help mobile app developers provide composite security and privacy features, instead of separate features, resulting in lower cost, time, and effort to provide secure mobile apps.

Against this backdrop, information system (IS) researchers have investigated security and privacy perceptions in different mobile technology contexts. For example, Johnson, Kiser, Washington, and Torres (2018) examined the predictors of mobile payment usage intentions and found that perceived security has a positive impact on user intentions towards mobile payment services. Keith, Babb, Furner, Abdullat, and Lowry (2016) conducted a cost-benefit analysis to examine drivers and inhibitors of mobile app adoption, finding that privacy risks inhibit users from adopting and disclosing information to mobile apps. Prior research has also noted that, although security and privacy are distinct, they are interrelated and affect each other (Smith, Dinev, & Xu, 2011). Bansal (2017) argued that security is concerned with protection and privacy is concerned with governance and use, but more work is needed to understand the relationship between these concepts. However, the relationship between security and privacy in the mobile app context has received little attention and is limited to examining the effects of one privacy-related construct on security perceptions in the adoption model (e.g., Johnson et al., 2018) or the information disclosure model (Nikkhah and Sabherwal, 2017a; Nikkhah, Balapour, and Sabherwal, 2018). Thus, we extend this idea and crystalize the relationship between security and the privacy perceptions of mobile apps in a single nomological network. This helps mobile security and privacy researchers to clearly relate the security and privacy perceptions of mobile apps and examine them appropriately in their studies.

This study builds upon the CPM theory (Petronio, 2002) to address the research question: *do privacy perceptions impact users' perceptions of mobile apps' security?* This research contributes to security and privacy literature, as we investigate the effects of privacy perceptions on security perceptions in the context of the information sensitivity of mobile apps. As prior research found that users have different privacy perceptions when working with less or more sensitive information (Li, Sarathy, & Xu, 2011; Malhotra, Kim, & Agarwal, 2004), this study explicitly includes the moderating effect of information sensitivity in the research model. This aims to determine whether the relationship between privacy and security perceptions differs for mobile apps that use less sensitive information (e.g., notetaking apps) and those that use more sensitive information (e.g., mobile-banking apps). Therefore, two separate studies were conducted to investigate the moderating effects of information sensitivity on the effects of privacy on security. Further, mobile app developers provide privacy policies to inform users of their fair information practices and provide assurances that the app will protect users' data and will not behave opportunistically. Users are able to see privacy policy statements on app marketplaces (e.g., App Store, Google Play) before downloading the app, or are prompted by app developers after installation to view and accept any new privacy policy updates. However, there is a need for more investigation on the effectiveness of privacy policy presence on mobile apps in the two contexts of less sensitive and more sensitive apps that are part of this study's objectives.

This study begins by reviewing existing security and privacy studies and identifying the main findings in these areas. Then, a research model based on CPM theory is proposed and is tested with two surveys – one for apps accessing less sensitive information (n = 487) and the other for apps accessing more sensitive information (n = 559). Subsequently, the results of hypotheses testing with covariance-based structural equation modeling (CB-SEM) are presented and the paper concludes with a discussion of research and practice implications.

2. Background

2.1. Mobile security perceptions

Users' behavioral security has been studied in numerous contexts in IS research, such as mobile technologies (Harris et al., 2016; Johnson et al., 2018; Keith, Babb, Lowry, Furner, & Abdullat, 2015), computer security (Johnston & Warkentin, 2010), internet security (Chen & Zahedi, 2016), online shopping (Pavlou, Liang, & Xue, 2007), and online transactions (Chellappa, 2008; Kim, 2008). Here, the focus is on security perceptions, which is the central construct in the behavioral stream of research on security because it affects user intentions and behaviors (Pavlou et al., 2007; White, Ekin, & Visinescu, 2017). By extension, we define the *perceived security* of mobile apps as the perception of the app provider's appropriate actions to safeguard shared information from security breaches during and after transmission through the mobile phone (Bansal, 2017; Johnson et al., 2018; Pavlou et al., 2007). By understanding the factors that affect mobile app users' perceived security, this study contributes to the ongoing conversation in the literature on behavioral security.

One of the issues that online shopping websites face, especially in their early stages, is the lack of user trust in the security of the website. Customers must share their financial information with the website, which can be abused by the website if not guarded well (Kim, 2008; Pavlou et al., 2007). Users' perceptions of security of can affect their attitude and behaviors directly and indirectly. For example, Chellappa (2008) and Bansal (2017) demonstrated that an individual's perception of security is the building block of trust (indirect) towards any form of electronic transaction, which can fuel users' behavioral intentions (direct), such as their intention to share private information with websites (Bansal, Zahedi, & Gefen, 2015). With a slightly different perspective, Kim, Steinfield, and Lai (2008) found that web assurance seal services can considerably mitigate users' security concerns. There are studies that specifically examine how an individual's perceptions of security can trigger coping and compliance behaviors. Examples of coping behaviors include avoidance, protective actions, and seeking help, which justify the motivations behind individuals' self-protection in online environments (Chen & Zahedi, 2016). For instance, Johnston and Warkentin (2010) indicated how security perceptions can indirectly lead to organizational security compliance, which is a significant problem in many companies.

To the best of our knowledge, few studies have focused specifically on the role of perceived security in the mobile app context. For example, Johnson et al. (2018) showed that perceived security affects the usage intentions of individuals in an empirical study of mobile payment apps. They showed that the perceived security of the mobile payment could be a function of the perceived privacy risk, ubiquity (user exposure to similar or the same thing), and trialability (having the opportunity to experiment with the technology; Johnson et al., 2018. Susanto, Chang, and Ha (2016) demonstrated that mobile security perception plays an important role in shaping user trust and satisfaction in mobile banking apps. Along similar lines, Ooi and Tan (2016) showed that security perception is the key influencer of behavioral intentions to use mobile app features, such as smartphone credit cards. However, research on the factors that impact user perceptions of mobile app security is sparse and, therefore, is studied here.

2.2. Mobile privacy perception

The functionality of many apps is overshadowed because of users' privacy concerns when using such apps (Keith et al., 2016). We define *perceived information privacy* in the mobile app context as the ability of the individual to control when, how, and to what extent, their personal information is communicated to mobile apps (Hong & Thong, 2013). In this study, the exposure of private information through unauthorized access, such as hacking incidents, is viewed as a security incident and discussed in Section 2.1. In this section, the concerns over privacy exposure focus on inappropriate use or misconduct by the app providers.

Users' privacy concerns are salient in the data collection and control processes that businesses exercise when managing shared data (Malhotra et al., 2004). By extension, recent work suggests that privacy concerns can be viewed as a multi-dimensional construct that consists of awareness about current privacy practices, information management by the party with whom they share personal information, and interaction management between the user and the third party (Hong & Thong, 2013). An individual's privacy perceptions will affect their behavior and attitudes, such as trust, willingness to use, intention to use, and intention to disclose information (Dinev et al., 2006; Lowry, Cao, & Everard, 2011; Malhotra et al., 2004; Smith et al., 2011; Xu, Teo, Tan, & Agarwal, 2009). Studies on the privacy paradox have also found that customers (or individuals in general) who seek more information transparency are less inclined to disclose information about themselves (Awad & Krishnan, 2006; Norberg, Horne, & Horne, 2007; Xu, Dinev, Smith, & Hart, 2011).

Existing studies have shown that privacy can directly or indirectly influence user attitudes and decisions to use mobile apps or share personal information with them. Wottrich, van Reijmersdal, and Smit (2018) found that the perceived privacy concerns of mobile app users in Western Europe negatively influenced their intentions to approve app permission requests to access their personal information. It has been demonstrated in multiple studies that both general perceived privacy concerns and perceived privacy risks directly and indirectly influence users' willingness to disclose personal information (e.g., identification, location, photos) to mobile apps (Xu et al., 2009), intention to pay to mobile apps (Keith, Thompson, Hale, Lowry, & Greer, 2013; Keith, Babb, Lowry, Furner, & Abdullat, 2015; Keith et al., 2016), and intention to adopt mobile apps (Luo, Li, Zhang, & Shim, 2010). The next sub-section provides an overview of the connection between privacy and security in IS research.

2.3. Interconnection of privacy and security

Privacy and security concerns are mutually exclusive, yet they affect each other (Smith et al., 2011), and are both very sensible for customers in online transactions (Pavlou et al., 2007). In IS research, privacy has been studied independently and in conjunction with security (Pavlou et al., 2007). It appears that both are equally important, particularly if sensitive information is being transferred between parties (Bansal & Zahedi, 2014). Kim (2008) studied the effects of security and privacy, at the individual and the collective level, on trust in e-vendors. He found that security positively influences trust on both levels, but privacy affects trust negatively only on the individual level. Kim et al. (2008) found that security is the main predictor of seal service awareness, but privacy is not. Roca, García, and de la Vega (2009) found a similar result to Kim et al. (2008), by testing the effects of both privacy and security perceptions on trust among users of online trading systems. Bansal and Zahedi (2014) advanced the idea of the effects of security and privacy concerns on trust, finding that each behaves differently in altered experimental conditions.

It has been established that in e-commerce transactions, user privacy perceptions positively influence their security perceptions (Chellappa, 2008). Shin (2010) demonstrated that users' perceptions of privacy on social network sites affects their security perceptions. Ponte, Carvajal-Trujillo, and Escobar-Rodríguez (2015) showed that the antecedents of privacy and security affect each other, identifying the need to further investigate the interaction between these two equally important constructs in privacy and security literature. Against this backdrop, this study assumes that privacy perceptions affect perceived security. Therefore, this study extends and contributes to the interconnection of privacy and security literature in the context of mobile apps.

2.4. Communication privacy management theory

This study draws on CPM theory, which explains the boundaries of self-disclosure within interpersonal relationships (Petronio, 2002). CPM theory (Petronio, 2002, 2008) posits that individuals draw implicit lines (boundaries) around themselves, to regulate the way their personal information is transacted. These boundaries overlap and are shared with third-parties associated with the individual (e.g., friends, family, co-workers, lawyers, physicians). The implicit rules and the degree of overlap between an individual's boundaries are very dependent on the social context and the type of information (Choi & Land, 2016). The underlying assumption of CPM is that individual ownership of information is the key factor in assessing whether to share personal information in transactions. The two parties involved in information disclosure can coordinate the use of the shared personal information. The mismanagement of shared personal information by either side can cause 'turbulence' (Acquisti, Brandimarte, & Loewenstein, 2015). Turbulence between the individual and the co-owner of the shared information occurs when the co-owner violates ownership expectations, and can frequently appear due to the complexity of the coordination process (Petronio, 2002; Xu et al., 2011).

IS researchers have adopted the CPM theory to investigate privacy-related phenomena in online settings. Anderson and Agarwal (2011) applied CPM to predict the factors that affect patients' willingness to provide access to personal health information. Xu et al. (2011) identified boundary management using CPM to predict the privacy concerns of users in web information transactions. Similarly, CPM has been applied to explain user intentions to disclose personal information to social networking sites (Choi & Land, 2016; Liu & Wang, 2018; Osatuyi, Passerini, Ravarini, & Grandhi, 2018; Walton & Rice, 2013). There are studies that partly adopted this theory to explain user behaviors, such as identifying perceived risk as forming the boundary to predict online community users' intentions to share information (Posey, Lowry, Roberts, & Ellis, 2010). In the mobile context, contemporary studies show that CPM theory is a useful lens for explaining the mobile commerce activities of app users based on their boundary management (Eastin, Brinson, Doorey, & Wilcox, 2016). Among the overarching theories in the areas of security and privacy, this study draws on CPM to explain the interaction of privacy-related concerns and security. As users are sharing their personal information with mobile app providers, the providers become the co-owner of users' private information. Consequently, CPM is helpful in explaining how individuals form their privacy boundaries and how they perceive the regulation of these boundaries by institutions (Liu & Wang, 2018; Xu et al., 2011).

3. Hypotheses

Fig. 1 summarizes the proposed research model, which is further explained in Sections 3.1 to 3.4. The model draws on CPM theory and the dependent variable is perceived mobile app security. This study relies on contemporary literature to identify boundary rule formation and boundary coordination and turbulence (Liu & Wang, 2018; Xu et al., 2011). The model proposes that some relationships will be different for users sharing more sensitive information with apps, such as banking and financial apps, compared to apps requiring less sensitive information, such as notetaking apps. Lastly, age and gender are used as control variables, based on prior studies on this topic (Lowry et al., 2011; Pavlou et al., 2007; Smith, Milberg, & Burke, 1996; Xu et al., 2011).

3.1. Boundary formation

Per CPM theory, the first step in understanding how individuals regard their privacy is to investigate how they establish their privacy boundaries (Petronio, 2002, 2008). As part of risk assessment, which happens in the early stages of boundary formation, individuals develop a perception of privacy risks associated with disclosing some private information to gain access to some promised benefits (Shaw & Sergueeva, 2019; Xu et al., 2011). For this reason, this study includes perceived privacy risk as a sub-set of boundary formation, which is proposed as being an important factor in the cost-benefit assessment of privacy boundary formation. In this context, perceived privacy risk is defined as the expected loss potential associated with releasing personal information to mobile apps (Malhotra et al., 2004; Xu et al., 2011).

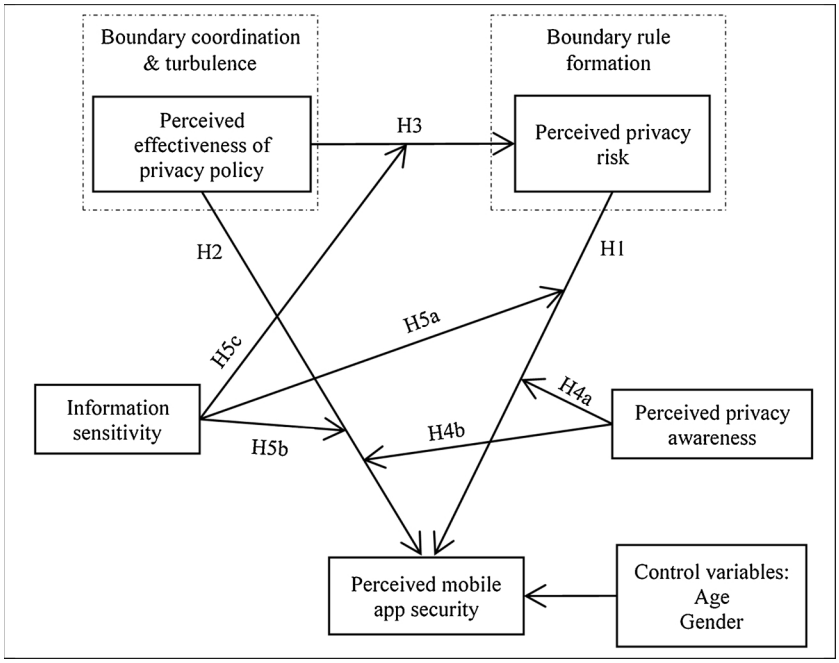

Fig. 1. Research model.

Examples of the personal information that apps request are: (a) location; (b) contact lists and calendars; (c) photos and videos; (d) microphone; and (e) credit card information (Wottrich et al., 2018). Allowing an app to access such personal information can jeopardize user privacy (King & Jessen, 2010) through the misuse of personal information, selling users' information to marketing and financial institutions without the users' permission,[1] insider disclosure, unauthorized access, and information theft (Dinev & Hart, 2006). In fact, mobile apps often make it mandatory for the user to share some private information to benefit from the basic functionalities of apps (Wottrich et al., 2018). On the other hand, users know that there is a chance of privacy invasion even with safeguards in place (Hong & Thong, 2013). Therefore, users must assess how the possible privacy risks would affect them when managing their privacy boundaries.

Prior studies have found that perceived privacy and security are distinct, but can affect each other (Bansal & Zahedi, 2014; Bansal, 2017; Chellappa, 2008). For example, Chellappa (2008) showed that the perceived privacy of e-commerce transactions positively influences the perceived security of these transactions. It has also been found that privacy risks affect the privacy perceptions of users (Dinev & Hart, 2006; Dinev et al., 2006; Dinev, Xu, Smith, & Hart, 2013; Liu & Wang, 2018; Xu et al., 2011). Given that the literature explicitly states a causal chain relationship between the discussed concepts, we posit that privacy risks and security are connected. Contemporary literature has shown there is a relationship between the perception of privacy risks and perceived security. For example, Johnson et al. (2018) showed that the perceived privacy risks of using mobile payment apps negatively impacts users' perceptions of the security of such apps. This study expands this argument and posits that users of any type of mobile app associate the risk of losing data through the mobile app with the security of the app. In other words, users perceive the security of mobile apps to be weak when they perceive a high probability of losing data. Thus, we hypothesize:

H1. The perceived privacy risk of using mobile apps negatively influences the perceived security of mobile apps.

[1] The Cambridge scandal of Facebook in 2018 is a great example of user personal information being sold to or shared with an analytical company without the users' awareness (BBC, 2018).

3.2. Boundary coordination and turbulence

Boundary coordination and turbulence is the other aspect of CPM theory (Petronio, 2002, 2008). This aspect addresses how the shared information will be coordinated and handled if any issues arise (e.g., data breaches). When users share private information with mobile apps, the mobile apps become the co-owner of the data. Therefore, by clearly describing how user information will be managed (i.e., in privacy policy statements), the app providers coordinate boundary rules with the users (as the co-owners of data) and state how to cope with boundary turbulence situations, such as unauthorized information disclosure. In fact, privacy policies often consist of the app providers' assurance practices to protect users' personal information, and the practices recommended by industry regulations and government laws (Privacypolicies, 2018). As a result, privacy policies can inform users about the use and process of their information (boundary coordination) and are the means of recourse in case of unauthorized disclosure (boundary turbulence). The privacy policy of Amazon's mobile app states that users' personal information will be used for or shared with: (a) affiliated businesses that they (Amazon) do not control; (b) third-party service providers; (c) promotional offers; and (d) business transfers. Amazon also discusses how the information will be gathered (e.g., automatic, mobile, email) and what their security measures are (e.g., revealing only the last four digits of credit cards on accounts and using SSL software to add layers of encryption; Amazon, 2017).

To capture users' perceptions of boundary coordination and turbulence, contemporary research has used the *effectiveness of privacy policies,* which refers to the extent to which a user believes that the privacy notice shown on the mobile app provides accurate and reliable information about the mobile app's information privacy practices (Liu & Wang, 2018; Xu et al., 2011). Although there are arguments that users do not read privacy policies, research has shown that privacy policies matter to users for privacy decision making (Tsai, Egelman, Cranor, & Acquisti, 2011). In general, in the US, which hosts many of the leading tech companies, privacy policies are built around the US Federal Trade Commission's Act. This includes five principles of fair information practice – notice, choice, access, security, and enforcement (Bansal et al., 2015; Wu, Huang, Yen, & Popova, 2012). Therefore, privacy policies include information about collecting and controlling user information, as well as information about security practices in place to protect users' data, which addresses user concerns and

promotes a positive attitude toward the effectiveness of the privacy policies. Prior research has found that when users perceive privacy policies to have a high effectiveness, they perceive mobile apps to be secure (Nikkhah and Sabherwal, 2017a, 2017b; Nikkhah, Balapour et al., 2018, Nikkhah, Grover, & Sabherwal, 2018). Similarly, we argue that when users believe that information on protective practices in a mobile app's privacy policies is reliable and accurate, they have a higher perception of the security of the app. Thus, we propose that:

H2. The perceived effectiveness of the privacy policy of mobile apps positively influences the perceived security of mobile apps.

As discussed earlier, privacy policies mitigate users' privacy concerns because they incorporate "assurance cues" that reduce the risk of losing information through the use of mobile apps (Bansal et al., 2015). They address users' concerns about the risk of online information transaction, by stating (a) what personal information is collected from users, (b) the accuracy and completeness of the data collection process, and (c) whether and how the collected information may be used for other purposes (Bansal et al., 2015). Given recent studies show that privacy policies influence user perceptions of privacy risk in different online settings (Chang, Wong, Libaque-Saenz, & Lee, 2018; Gerlach, Widjaja, & Buxmann, 2015; Xu et al., 2011), we argue that when users feel assurance practices in the privacy statements of mobile apps are fair and effective, they perceive a lower risk of working with mobile apps. Thus, we posit that:

H3. The perceived effectiveness of a privacy policy is negatively associated with the perceived privacy risk of mobile apps.

3.3. Privacy awareness

One of the reasons why individuals have different privacy concerns about the same phenomena is their varying levels of privacy awareness. For example, Smith et al. (2011) argue that individuals who are aware that some websites and applications may collect their personal information without their permission have more privacy concerns than individuals who are not aware of such malicious activities. Privacy awareness refers to the degree to which a person is aware of information privacy practices in general and the use of this by mobile apps (Malhotra et al., 2004). To illustrate, an individual's privacy awareness is increased by reading and watching news, reading books and magazines, and hearing about privacy issues from friends or other people within their social bubble. In effect, privacy awareness can influence an individual's attitude and perceptions toward mobile apps (Li et al., 2011).

Privacy awareness exerts an influence on privacy-related perceptions because an individual's awareness stimulates their protective behaviors (Smith et al., 2011). The difference in users' levels of privacy awareness leads to different privacy and security perceptions of mobile apps (Acquisti & Gross, 2006). Therefore, privacy awareness increases or decreases the strength of the relationship between privacy-related concerns and security. For example, users with a higher level of privacy awareness perceive mobile apps to have lower security because they have read or heard more about unauthorized information disclosure incidents and know that such incidents transpire frequently with less secure mobile apps. Similarly, users with a higher level of privacy awareness assume that privacy policy statements that incorporate privacy and security practices are not necessarily an indicator of the higher level of mobile app security, due to the prevalence of privacy and security incidents despite the providers' protection efforts. Thus, we hypothesize that:

H4a. A user's perceived privacy awareness moderates the effect of perceived privacy risk on the perceived security of apps, such that the relationship is stronger when perceived privacy awareness is high.

H4b. A user's perceived privacy awareness moderates the influence of the perceived effectiveness of the privacy policy on the perceived security of apps, such that the relationship is weaker when perceived privacy awareness is high.

3.4. Information sensitivity

Although there is a wide range of mobile applications (e.g., games, lifestyles, financial, utility, and education), the sensitivity of the information given to each app is different. Users have different privacy and security perceptions toward information disclosure based on the type of information shared with each app. That is, individuals are more concerned about releasing information to financial apps than fitness or game apps. Malhotra et al. (2004) argue that users have different levels of concerns when sharing more sensitive information, finding that when users are requested to provide more sensitive information, they perceive a higher risk and have lower intentions to disclose the requested information. Despite the importance of information sensitivity in privacy research, prior research on mobile apps does not consider the effect of information sensitivity on privacy-related relationships (Keith et al., 2016; Nikkhah & Sabherwal, 2017a; Xu et al., 2009). This study fills this gap by categorizing mobile apps as more sensitive information apps (e.g., financial apps) and less sensitive information apps (e.g., notetaking apps).

In general, sharing more sensitive information with mobile apps causes users to be more concerned, because if the shared information is disclosed to third-parties, users must deal with consequences that can disrupt their daily lives.[2] When users are required to provide more sensitive information, they become more conscious of the consequences of disclosing information to mobile apps. When a mobile app requests access to the mobile device's location service, to track users' locations, users focus more attention on giving such permission (Keith et al., 2016; Xu et al., 2009). Thus, users with the same perceptions of privacy risk perceive mobile apps that request more sensitive information to have lower security, because they expect these apps to be more secure than apps requesting less sensitive information. For instance, users expect financial apps to be more secure than games, but when users perceive the same level of risk with financial apps and games, they perceive financial apps to have lower security. With the same logic, when users are required to provide more sensitive information, the presence and understanding of a privacy policy becomes more important and users consider the privacy policy more. Hence, the effect of a privacy policy on the risk and security perceptions of mobile apps becomes stronger when users need to provide more sensitive information. Prior privacy studies have considered the moderating role of information sensitivity in privacy-related relationships and found that perceptions pertain to information disclosure changes when users disclose more sensitive information (Okazaki, Li, & Hirose, 2009). As a result, we consider the moderating role of information sensitivity and hypothesize that:

H5a. Information sensitivity moderates the relationship between perceived privacy risk and the perceived security of mobile apps, such that the relationship is stronger with more sensitive information.

H5b. Information sensitivity moderates the relationship between the perceived effectiveness of privacy policies and the perceived security of mobile apps, such that the relationship is weaker with more sensitive information.

H5c. Information sensitivity moderates the relationship between the perceived effectiveness of privacy policies and the perceived privacy risk of mobile apps, such that the relationship is stronger with more sensitive information.

4. Methods and data

We published two independent web-surveys on Amazon Mechanical Turk to reach a large sample of mobile app users of different genders,

[2] For example, unathorized disclosure of sensitive information, such as a social security number and credit card information, can lead to identity theft and financial loss.

education levels, and age groups in the US, similar to prior studies on privacy and security perceptions (Dinev & Hart, 2006; Dinev et al., 2013; Hong & Thong, 2013; Lowry et al., 2011; Malhotra et al., 2004; Xu et al., 2011). The selection of Amazon Mechanical Turk for participant sampling has theoretical validity, as it is a sample of consumers or regular users and not specialized employees or individuals (Jia, Steelman, & Reich, 2017). We adapted the items in the survey from previously validated measures. Perceived security items were based on measures developed by Chellappa (2008). The measures of perceived privacy risk and perceived privacy awareness were adopted from Malhotra et al. (2004), and the measures of effectiveness of privacy policies were adopted from Xu et al. (2011). Seven-point Likert scales, with anchors ranging from 'strongly disagree' to 'strongly agree', were used for all items.

Before conducting the primary study, we conducted a pilot study to solicit feedback and revise the questions as necessary. Two IS researchers and four IS PhD students[3] reviewed the instruments and assessed the length of the survey, the format, the face validity of the scales, and the clarity of the questions. We modified some of the questions to improve clarity, based on the pilot study feedback. The primary study involved launching two surveys on Amazon Mechanical Turk, with different wording, to target users of apps that collect more sensitive information and users of apps that collect less sensitive information. We asked the participants of the more-sensitive group whether they use or have used any mobile banking apps, such as Bank of America, Citibank, and Chase (this allowed us to remove participants who had never used or interacted with banking apps). Next, the participants were asked to consider their own banking app or one of the example mobile banking apps while answering the questions. For the less-sensitive group, we focused on one particular app, called Evernote,[4] which is a notetaking app. We asked participants whether they use Evernote, to automatically preclude participants who had no experience using Evernote from participation. Then, the participants were asked to consider Evernote while answering the questions.

We encouraged participation in our study by using a small monetary incentive. Table A1 shows the survey for the more sensitive group. We replaced the references to mobile banking apps with references to Evernote for the less sensitive group. Mobile banking apps have access to users' identification and financial information, home addresses, contact details, and social security numbers, while notetaking apps, such as Evernote, only request limited information from users. Overall, we received 1544 responses (all US participants) to both surveys, removing incomplete responses and those that were completed in under five minutes (Jia et al., 2017). We received 1046 usable responses, including 559 from the more sensitive group and 487 from the less sensitive group. Table 1 summarizes the demographics of the study participants.

5. Analyses and results

5.1. Preliminary data analysis

First, we separately examined the content validity, construct validity, and reliability of the constructs based on prior recommendations for each sample (Straub, Boudreau, & Gefen, 2004). Tables 2 and 3 show the means and standard deviations, and the reliability, validity, and correlation results for the constructs. By adopting previously validated instruments, we assured content validity. In addition, Tables 2 and 3 show that Cronbach's alpha, as well as the composite reliability, for all four constructs are above 0.7, which supports the reliability of the constructs (Hair, Anderson, Tatham, & Black, 2013). For construct validity, we assessed the convergent and discriminant validity. The loadings of the construct items are above 0.7 (Table A1) and the values of the average variance extracted (AVE) are above 0.5, supporting convergent validity (Hair et al., 2013). Tables 2 and 3 show the square roots of all AVEs exceed all correlations among the constructs and the results of the principal component analysis show no cross-loadings above 0.4 (Table B1), indicating the discriminant validity of the constructs (Fornell & Larcker, 1981).

Next, we conducted Harmon's one-factor test to examine common method variance (Gefen, Straub, & Boudreau, 2000; Hair et al., 2013). All 12 items were loaded on a single factor. The results show that the single factor explains 43 % (for the more sensitive sample) and 40 % (for the less sensitive sample) of the total variance, suggesting that there is no common method bias in the samples.

5.2. Measurement model

The measurement model meets the recommended fit indices (Fornell & Larcker, 1981; Gefen et al., 2000; Hair et al., 2013; Hu & Bentler, 1999). For the more sensitive sample, the fit indices are as follows: comparative fit index (CFI) = 0.97; Tucker-Lewis index (TLI) = 0.96; root mean squared error of approximation (RMSEA) = 0.057; standardized root mean squared residual (SRMR) = 0.043; χ^2/degree of freedom = 2.79 (d.f. = 63; $p < 0.001$); N = 559. For the less sensitive sample, the fit indices are as follows: CFI = 0.99; TLI = 0.99; RMSEA = 0.025; SRMR = 0.021; χ^2/degree of freedom = 1.30 (d.f. = 62; $p < 0.001$); N = 487. CFI and TLI should be above 0.90; SRMR and RMSEA should be under 0.08. All of the indices meet the recommended thresholds and are satisfactory.

5.3. Structural model

To test the proposed model, we used covariance-based structural equation modeling (CB-SEM), with the maximum likelihood method, in Sata 15.1. Fig. 2 presents the results of the final structural model. As there are continuous and categorical moderating variables in our model, we used different approaches to estimate the moderating effects. First, we used Lin et al.'s (2010) technique, known as double mean-centering, to estimate the moderating effects of privacy awareness, as this is a continuous variable (Cortina, Chen, & Dunlap, 2001; Lin, Wen, Marsh, & Lin, 2010). Correspondingly, we mean-centered all the items associated with perceived privacy risk, perceived effectiveness of privacy policies, and perceived privacy awareness. Then, we created interactions of the observed variables through the matched pair product indicator strategy (Marsh, Wen, & Hau, 2004), by matching items two-by-two and multiplying them (i.e., multiplying each matched PA item in the respective PPE and PR items). Three new items for each interaction construct were generated.[5] Finally, we mean-centered the three generated items and used the results as indicators of the three latent constructs for the interactions. The matched pair strategy provides similar results to the all pair strategy, in which nine items are generated through three by three multiplications, but the matched pair approach enables simplicity and better fit indices (Foldnes & Hagtvet, 2014; Marsh et al., 2004). Second, to test the moderating effects of information sensitivity as the categorical variable, we compared the beta-coefficient of the model in each sample using a z-test to examine if the path coefficients were significantly different.

Table 4 provides the results that show all fit indices meet the recommended values (Gefen et al., 2000). The results for both models (model 1: more sensitive information sample; model 2: less sensitive

[3] The assumption was that people with an IS background are more familiar with topics such as privacy and security, thus they could provide better feedback on the technical aspect of the survey and the study design.

[4] This app was selected for three reasons – (1) it does not collect sensitive information from users; (2) it is an app the authors are familiar with and know more about than other similar apps; (3) it was fairly easy to reach out to users of this app on Amazon Mechanical Turk.

[5] PA1 × PPE1, PA2 × PPE2, PA3 × PPE3 for creating items of *Privacy Awareness* × *Effectiveness of Privacy Policy*; PA1 × PR1, PA2 × PR2, PA3 × PR3 for creating items of *Privacy Awareness* × *Privacy Risk*.

Table 1
Respondent demographics.

Demographic variables	Category	More sensitive: Frequency (Percentage)	Less sensitive: Frequency (Percentage)
Gender	Male	323 (57.78)	228 (46.82)
	Female	236 (42.22)	259 (53.18)
Age	20 and under	18 (3.22)	7 (1.44)
	21-30	199 (35.60)	200 (41.07)
	31-40	173 (30.95)	148 (30.39)
	41-50	93 (16.64)	65 (13.35)
	Over 50	76 (13.60)	67 (13.76)
Education	High school or equivalent	253 (45.26)	207 (42.51)
	Bachelor	216 (38.64)	207(42.51)
	Master	73 (13.06)	60 (12.32)
	Doctorate equivalent or above	17 (3.04)	13 (2.67)

Table 2
More sensitive information app users: Descriptives, Reliabilities, Average Variance Extracted, and Correlations.

	Mean	S.D.	CR	α	AVE	1	2	3	4	5	6
1. Gender (male = 0)	0.42	0.49	–	–	–	–					
2. Age	36.05	11.56	–	–	–	−0.02	–				
3. PA	6.58	0.54	0.79	0.78	0.56	−0.02	0.06	0.75			
4. PR	3.71	1.36	0.89	0.88	0.73	−0.03	0.16**	0.12**	0.85		
5. PPE	5.17	1.14	0.94	0.88	0.78	−0.06	−0.13**	0.10**	−0.51**	0.88	
6. PS	4.75	1.14	0.82	0.83	0.62	−0.08*	−0.20**	−0.02	−0.61**	0.66**	0.79

S.D. = Standard deviation; CR = Composite Reliability; α = Chronbach's Alpha; PA = Privacy Awareness; PR = Privacy Risk; PPE = Perceived Effectiveness of Privacy Policy; PS = Perceived Security.
** $p < 0.01$.
* $p < 0.05$. The diagonal represents the square root of the AVE.

Table 3
Less sensitive information app users: Descriptives, Reliabilities, Average Variance Extracted, and Correlations.

	Mean	S.D.	CR	α	AVE	1	2	3	4	5	6
1. Gender (male = 0)	0.53	0.49	–	–	–	–					
2. Age	35.60	11.48	–	–	–	0.15**	–				
3. PA	6.09	1.04	0.87	0.91	0.71	0.16**	0.22**	0.84			
4. PR	4.89	1.23	0.90	0.90	0.76	0.01	0.17**	0.27**	0.87		
5. PPE	4.40	1.28	0.94	0.92	0.79	0.11*	−0.05	−0.01	−0.22**	0.89	
6. PS	4.14	1.30	0.91	0.90	0.77	−0.02	−0.14**	−0.10*	−0.31**	0.66**	0.87

S.D. = Standard deviation; CR = Composite Reliability; α = Chronbach's Alpha; PA = Privacy Awareness; PR = Privacy Risk; PPE = Perceived Effectiveness of Privacy Policy; PS = Perceived Security.
** $p < 0.01$.
* $p < 0.05$. The diagonal represents the square root of the AVE.

information sample) suggest that the perceived privacy risk negatively affects the perceived security of mobile apps (β_1 = -0.25; β_2 = -0.17, $p < 0.01$), supporting H1. The results suggest that the perceived effectiveness of privacy policies positively affects the perceived security of mobile apps (β_1 = 0.63; β_2 = 0.68, $p < 0.01$) and negatively affects the perceived privacy risk (β_1 = -0.61; β_2 = -0.23, $p < 0.01$), which supports H2 and H3.

The results show that perceived privacy awareness moderates the effect of perceived privacy risk on the perceived security of mobile apps for both groups of app users (β_1 = -0.10; β_2 = -0.08, $p < 0.1$). So, H4a is supported. However, the results did not show the moderating effect of privacy awareness on the relationship between the perceived effectiveness of privacy policies and the perceived security of mobile apps across both samples (β_1 = -0.02, p = 0.72; β_2 = -0.01, p = 0.97). So, H4b is not supported. Fig. 3 exhibits the interaction effect between privacy awareness and privacy risk, which shows that when the perceived privacy risk is high, a higher privacy awareness causes the user to have a lower level of perceived security. Findings suggest that age negatively influences the perceived security of more sensitive information apps (β_1 = -0.08, $p < 0.01$). However, results did not show such an effect for less sensitive apps (β_2 = -0.05, p = 0.12). The results demonstrate that gender plays a reverse role for each group of app users, which means gender was positively associated with perceived security for sensitive app users (β_1 = 0.10, $p < 0.01$). In contrast, gender was negatively associated with perceived security for less sensitive app users (β_2 = −0.09, $p < 0.01$).[6]

Lastly, this study tested the moderating effect of information sensitivity by comparing the beta-coefficient of the estimated models

[6] The influence of gender is interpreted this way: (1) for more sensitive app users, one unit change in gender (from male = 0 to female = 1) accounts for + 0.10 unit change in the perceived security; (2) for less sensitive app users one unit change in gender (from male = 0 to female = 1) accounts for - 0.09 unit change in the perceived security. Further explanation is provided in the discussion section.

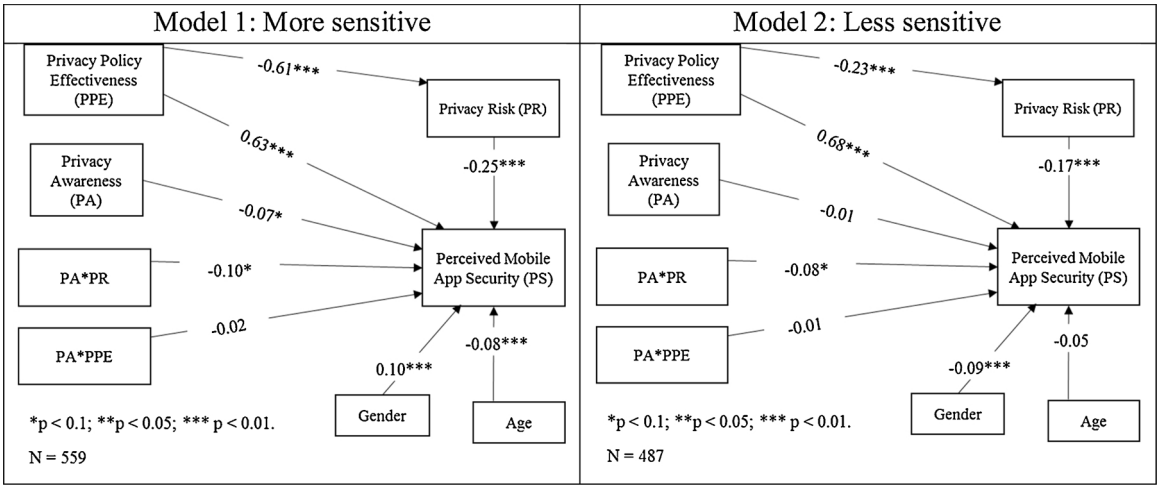

Fig. 2. Results of analysis for both groups.

Table 4
Results of analysis.

		Model 1 (More sensitive)	Model 2 (Less sensitive)	Coefficient comparison (z-test)	Cohen's d (effect size)
Path Coefficients:	PPE→PR	−0.61***	−0.23***	9.40***	0.47
	PR→PS	−0.25***	−0.17***	2.01**	0.10
	PA→PS	−0.07*	−0.01	1.36	0.06
	PPE→PS	0.63***	0.68***	1.22	0.05
	PA × PR→PS	−0.10*	−0.08*	0.41	0.01
	PA × PPE→PS	−0.02	−0.01	0.32	0.01
Covariates:	Age→PS	−0.08***	−0.05	0.85	0.05
	Gender→PS	0.10***	−0.09***	−6.07***	0.37
Fit Indices:	N	559	487	–	–
	χ^2 (d.f.)	402.71 (140)***	373.07 (146)***	–	–
	CFI	0.95	0.96	–	–
	TLI	0.94	0.95	–	–
	RMSEA	0.06	0.06	–	–
	SRMR	0.05	0.08	–	–

N = Sample size.
PPE = Perceived Effectiveness of privacy policy; PR = Perceived privacy risk; PS = Perceived security.
Note: The coefficient comparison was done using a z-test to see whether the type of mobile app (more sensitive vs. less sensitive) affects the strength of relationships.
* p < 0.1.
** p < 0.05.
*** p < 0.01.

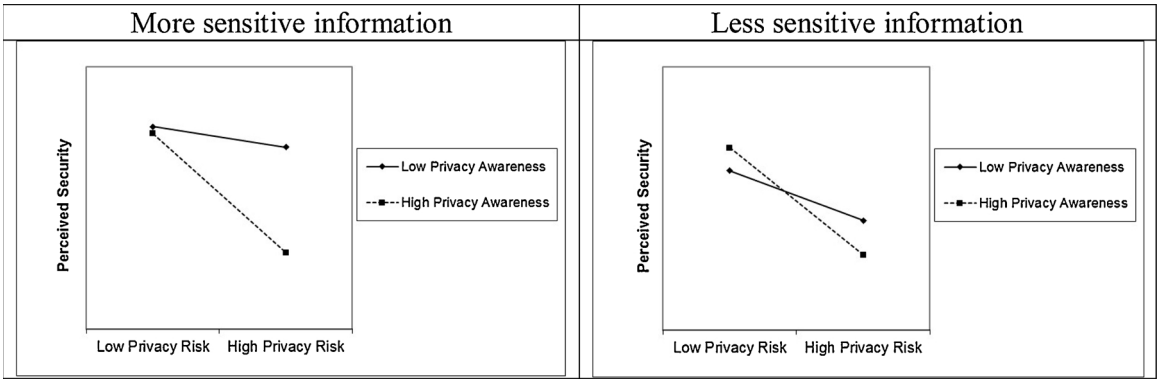

Fig. 3. Interaction plots.

(model 1 versus model 2). As Table 4 shows, the results do not indicate any moderating effects of app type on the relationship between perceived risk and perceived security (z = 1.52, d.f. = 1044, p = 0.13), or between the perceived effectiveness of privacy policies and perceived security (z = 0.83, d.f. = 1044, p = 0.41). Therefore, H5a and H5b are not supported. However, the type of apps being used affects the strength of the relationship between the perceived effectiveness of privacy policies and perceived risk, such that the relationship is stronger when an app collects and transmits more sensitive information (z = 7.62, d.f. = 1044, p < 0.01). Hence, H5c is supported. A surprising finding regarding information sensitivity is its effect on the relationship between gender and perceived security. Results showed that the effect of gender on perceived security is stronger for users of more sensitive information apps (z = -5.89, d.f. = 1044, p < 0.01).

6. Discussion

Mobile apps have become ubiquitous in everyday life, which has led mobile app developers to persistently provide new apps to meet users' evolving needs. However, user security concerns are a barrier to the diffusion of mobile computing technologies, including mobile apps (Lin, Huang, Wright, & Kambourakis, 2014). This study used CPM theory (Petronio, 2002, 2008) to predict how privacy concerns regarding mobile apps affect users' security perceptions. By extension, a research model was proposed in which perceived privacy risks represented the boundary rule formation of CPM and the perceived effectiveness of privacy policies represented boundary coordination and turbulence. The findings suggest that perceived privacy risk negatively affects the security perception of mobile apps, which is consistent with existing literature (Johnson et al., 2018). When users perceive that the risk of using the mobile app is higher than its benefits, they tend to perceive the app to be less secure. For instance, if exchanging personal information over a mobile communication app comes with high risks, then the user assumes this app is not as secure as it should be.

In addition, this study finds that privacy policies play a key role in predicting the perceived security of mobile apps. Prior studies found the effectiveness of a privacy policy decreases the perception of privacy risk for online banking customers (Chang et al., 2018) and general online web users (Wu et al., 2012), but such effect has not been examined in the context of mobile apps. In particular, the results suggest that when users perceive a privacy policy to be effective, they perceive fewer privacy risks inherent in the app and perceive a high level of security. There is little research that has studied the role privacy policies play in security perceptions, but the empirical findings of this study resonate with the fact that the privacy policies of mobile apps actively communicate the security strategies, precursors, and measures used to protect users' private data (i.e., Bank of America, 2018; Dropbox, 2018). So, when users perceive such policies to be effective, their security perception of the mobile app increases.

The results also show that users' perceived privacy awareness moderates the effect of perceived privacy risk on the perceived security of mobile apps. As shown in Fig. 3, under high privacy awareness conditions for both samples, the relationship between perceived privacy risk and the perceived security of mobile apps becomes stronger (the slope is steeper). When individuals increase their knowledge about privacy practices and issues, by reading and watching news, books, and privacy statements, they tend to be on high alert. It is difficult for these users to deem apps as secure, given the negative information in the media about the security of mobile technologies. Being aware of privacy and security practices is not a substitute for users knowing their information can still be compromised, even if the most rigorous privacy and security measures are in place (Hong & Thong, 2013).

The findings suggest that the user differences between more sensitive and less sensitive apps only exists for the relationship between the perceived effectiveness of privacy policies and the perceived privacy risk. When individuals use applications requiring sensitive information, such as mobile banking apps, the perceived effectiveness of the privacy policy has a greater effect on their perception of the privacy risk compared to the use of an app that requires less sensitive information, such as note-taking apps. Similarly, we observed a difference between the influence of perceived privacy risk on perceived security for both groups, which highlights that, for users providing more sensitive information, the perceived security risk is more dependent on the mitigation of privacy risks, compared to users providing less sensitive information.

However, no such difference across the groups was found for the relationship between the perceived effectiveness of privacy policies and the security of mobile apps. This suggests that, when it comes to risk mitigation, both groups see privacy policies as functioning equally in assuring that security measures are in place to protect the user. Li et al. (2011) suggest that information sensitivity affects some of the relationships (but not all) in a privacy-related study. In particular, they theorized that the sensitivity of information moderates the effect of users' perceived information relevancy on privacy risk belief.

The results also indicate that age negatively influences perceived security for users providing more sensitive information. This means that, as an individual's age increases, their security perception of mobile apps decreases. As age comes with experience, aged people may have experienced more security incidents, so could be less optimistic about the security of mobile apps. This could also be explained by the optimistic bias in younger people, which manifests in the form of having higher security perceptions. Surprisingly, gender has different effects on perceived security (model 1 vs. model 2). For the more sensitive group, being female was associated with having a higher perception of the security of mobile apps. However, for the less sensitive group, being female was associated with having a lower perception of the security of mobile apps.[7] Gender was positively associated with perceived security, whereas for the less sensitive group, it was negatively associated with the perceived security of mobile apps. The cross-group comparison revealed a statistically meaningful difference between the effect of gender on the perceived security of mobile apps across both groups. Overall, the results show that users' privacy concerns do affect their perceptions of the security of mobile apps, which can hinder their adoption and diffusion.

6.1. Implications for research and practice

The findings of this study have implications for both researchers and practitioners. The most important contribution of this paper is that privacy antecedents affect users' perceptions of security. Although security and privacy have been studied together or separately, to our knowledge, prior studies did not consider how the antecedents of privacy affect security, even though these concepts are related (as shown in this study). In practice, mobile app developers actively address security in their privacy policy statements, which demonstrates that these concepts and their antecedents are related (e.g. Dropbox); however, scientific conversation is lacking in the mobile apps context. Therefore, one of this study's objectives was to extend the scholarly discussion on the effects of behavioral privacy-related variables on behavioral security.

This study contributes to the ongoing debate regarding mobile threats and mobile security issues. Existing literature emphasizes that investing in technology to enhance security is not always the solution; there should also be an emphasis on teaching individuals to improve their security behaviors (White et al., 2017). Accordingly, this study investigated the factors that affect users' behavioral security. In many cases, mobile security incidents happen due to users' lack of knowledge or their use of insecure practices when using their mobile phone. In particular, this study shed light on the sensitive role of privacy policies in shaping users' privacy and security perceptions, which could be studied further in future studies. For example, a future research question could be: *what section(s) of a privacy policy statement are more effective for forming users' privacy and security perceptions?* Or *what are the characteristics of an effective privacy policy statement in users' minds?*

This study used CPM theory (Petronio, 2002, 2008) to propose a research model that predicts the effect of privacy perceptions on users' perceptions of mobile app security. By using the CPM theory, the results of testing the nomological model of privacy and security show that the effectiveness of privacy policies and privacy risk (two antecedents of privacy concerns) affect users' perceptions of mobile app security. Consequently, we encourage future researchers to adopt CPM to measure and explain security-related phenomena, as we have justified this theory as a good fit for explaining behavioral security.

The results of this study have implications for practice as well. Mobile app developers who are planning to develop or improve their apps should work towards using the potential of privacy policies, which (we found)

[7] This could also be examined from the male perspective: (1) for the more sensitive group, being male was associated with a lower perception of security; (2) for the less sensitive group, being male was associated with a higher perception of security.

reduces users' perceptions of privacy risk and affects users' security perceptions. By extension, institutions can provide guidelines within privacy policies to help users improve their security and privacy behaviors. Several examples of daily behavior that can potentially lead to privacy and security exposure, such as allowing children to download insecure gaming apps that request access to personal information, are often overlooked by parents. Privacy policies could also provide guidelines on password setting or common examples of fraudulent activities that users might not be aware of. Currently, app developers try to meet only the minimum standards of the security and privacy guidelines set by industry regulations, but they should take advantage of the privacy policy to educate users by providing examples of how security and privacy violations can happen.

The results of this study show that privacy awareness moderates the effect of perceived privacy risk on the perceived security of mobile apps. Investing time and money into elevating users' awareness thorough different methods (such as privacy policies) would always help in preventing security incidents and unwanted privacy disclosures. There are benefits for companies in raising users' awareness, such as contributing to the creation of a safer and more secure business economy, which is beneficial to both businesses and customers. The results have shown that there is a significant difference in the effect of privacy policies on privacy risk in more sensitive and less sensitive contexts. This shows that, if the privacy policies for more sensitive mobile apps (i.e., mobile banking apps) address the security strategies and preventive measures in place, users perceive fewer risks, compared to less sensitive mobile apps. App developers should provide more information about data collection and protective measures in more sensitive apps, because this affects user perceptions of privacy risks.

6.2. Limitations

The results of this study should be viewed in light of its limitations. First, although the findings generally support the hypotheses, this study did not extend the model to include the outcomes of perceived security that could be translated into variables, such as intention to use. We encourage future researchers to go beyond the proposed model by integrating other privacy (e.g., privacy control and privacy experiences; Smith et al., 2011; Xu et al., 2011) and security-related variables (e.g., perceived threat severity and perceived threat vulnerability; Bélanger, Collignon, Enget, & Negangard, 2017), and even extend the model by involving other outcome variables deemed suitable.

Both samples collected for this study were limited to one method – a questionnaire survey. Even though the use of two groups increased the generalizability of the findings, existing method studies emphasize triangulation and the use of multiple methods (Orlikowski & Baroudi, 1991). Survey data has potential issues, such as common method bias and high measurement errors (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003; Straub et al., 2004). We addressed the common method bias, but there are other data sources (i.e., archival data) that are less prone to such issues and biases. This study did not have access to such sources, but we encourage future researchers to look for other sources, such as log data, to better predict the security behavior of app users.

7. Conclusion

This paper addressed the following research question: *do privacy perceptions impact users' perceptions of mobile apps' security?* Unlike the prior literature, which only tested the effect of privacy on security or vice versa, this study examined the effect of privacy antecedents on users' security perceptions. More specifically, this paper examined whether privacy risk and the effectiveness of privacy policies, two antecedents of privacy concerns, affect the perceived security of mobile apps. The empirical results of this study suggest that the antecedents of privacy directly affect users' perceptions of security. Both boundary rule formation and boundary coordination and turbulence affect users' perceptions of security. The results show that privacy awareness moderates the effect of perceived privacy risk on perceived security. This study found that the effectiveness of privacy policies (boundary coordination and turbulence) affects privacy risk (boundary rule formation). Thus, this paper has provided some initial insights into the effects of the antecedents of privacy concerns on the perceived security of mobile apps. We hope that this paper can motivate future investigations into the complex effects of privacy on security, while testing whether the antecedents of these constructs affect each other.

Appendix A

Table A1
Measurements.

Items (first row for each construct pertains to the construct and sources for items are listed in parentheses next to each construct)	λ	Mean	St.d.	Cronbach's alpha
Perceived Privacy Awareness (Malhotra et al., 2004)	–	6.35	0.85	0.89
Companies seeking personal information online should disclose the way the data are collected, processed, and used.	0.88	6.35	0.94	–
A good mobile banking privacy policy should have a clear and conspicuous disclosure.	0.91	6.40	0.90	–
It is very important to me that I am aware and knowledgeable about how my personal information will be used.	0.79	6.30	0.97	–
Perceived Privacy Risk (Malhotra et al., 2004)	–	4.26	1.43	0.91
In general, it would be risky to give my personal information to mobile banking application ns.	0.88	4.38	1.53	–
There would be high potential for loss associated with giving my personal information to mobile banking applications.	0.85	4.44	1.55	–
Providing mobile banking applications with my personal information would involve many unexpected problems.	0.87	3.95	1.56	–
There would be too much uncertainty associated with giving my personal information to mobile banking applications.*	–	4.45	1.63	–
Perceived Effectiveness of Privacy Policy (Xu et al., 2011)	–	4.81	1.27	0.91
I feel confident that these mobile banking applications` privacy statements reflect their commitments to protect my personal information.	0.86	4.84	1.32	–
With their privacy statements, I believe that my personal information will be kept private and confidential by mobile banking.	0.94	4.85	1.39	–
I believe that these mobile banking applications` privacy statements are an effective way to demonstrate their commitments to privacy.	0.81	4.76	1.42	–
Perceived Security (Chellappa, 2008)	–	4.47	1.26	0.88
I am confident that the private information I provide during my transaction with mobile banking application system will only reach its system.	0.91	4.71	1.40	–
I believe inappropriate parties may deliberately view the information I provide during my transaction with mobile banking application system (Reversed).	0.76	4.15	1.39	–
I believe the information I provide during my transaction with mobile banking application system will not be manipulated by inappropriate parties.	0.82	4.55	1.40	–
I have confidence in the security of my transaction with mobile banking applications.*	–	4.39	1.41	–

Note: For the second survey, we changed mobile banking applications to Evernote.
* Dropped.

Appendix B

Table B1
Principal Component Analysis.

Loadings and cross-loadings.

Items	More sensitive users' sample				Less sensitive users' sample			
	PPE	PR	PA	PS	PPE	PS	PA	PR
PPE1	**0.56**	−0.06	0.00	−0.07	**0.60**	−0.03	0.01	−0.01
PPE 2	**0.51**	−0.02	−0.02	0.06	**0.52**	0.07	0.01	−0.01
PPE 3	**0.58**	0.05	0.03	−0.06	**0.60**	−0.02	−0.02	0.02
PR1	0.00	**0.59**	−0.02	0.00	0.05	−0.05	0.01	**0.58**
PR2	−0.01	**0.60**	0.03	0.06	0.02	−0.03	0.02	**0.57**
PR4	0.00	**0.51**	−0.03	−0.09	−0.07	0.08	−0.03	**0.58**
PA1	−0.03	−0.06	**0.60**	−0.02	−0.02	0.00	**0.59**	−0.03
PA2	0.02	−0.02	**0.59**	0.01	0.01	0.00	**0.59**	−0.02
PA3	0.03	0.11	**0.53**	0.01	0.01	0.00	**0.54**	0.06
PS2	0.26	0.03	−0.04	**0.40**	0.01	**0.57**	0.04	−0.01
PS3	−0.13	−0.08	0.04	**0.65**	−0.03	**0.59**	−0.03	0.01
PS4	0.04	0.08	−0.02	**0.63**	0.02	**0.56**	0.00	0.01

PPE = Perceived effectiveness of privacy policy; PR = Perceived privacy risk; PA = Perceived privacy awareness; PS = Perceived security of mobile app.

References

Acquisti, A., & Gross, R. (2006). *Imagined communities: Awareness, information sharing, and privacy on the facebook. International workshop on privacy enhancing technologies.* Berlin, Heidelberg: Springer36–58.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science (New York, NY), 347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465.

Amazon (2017). *Amazon privacy notice.* August 29 Retrieved fromhttps://www.amazon.com/gp/help/customer/display.html?nodeId=468496.

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research, 22*(3), 469–490. https://doi.org/10.1287/isre.1100.0335.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly, 30*(1), 13–28. https://doi.org/10.2307/25148715.

Balapour, A., Reychav, I., Sabherwal, R., & Azuri, J. (2019). Mobile technology identity and self-efficacy: Implications for the adoption of clinically supported mobile health apps. *International Journal of Information Management, 49*, 58–68.

Balapour, A., & Sabherwal, R. (2017). Usability of Apps and Websites: A Meta-Regression Study. *In: Proceedings of Americas Conference on Information Systems.* Retrieved from https://aisel.aisnet.org/amcis2017/HumanCI/Presentati.

Bank of America (2018). *Bank of America U.S. Online privacy notice.* May 1 Retrieved fromhttps://www.bankofamerica.com/privacy/online-privacy-notice.go.

Bansal, G. (2017). Distinguishing between privacy and security concerns: An empirical examination and scale validation. *Journal of Computer Information Systems, 57*(4), 330–343. https://doi.org/10.1080/08874417.2016.1232981.

Bansal, G., & Zahedi, F. M. (2014). Trust-discount tradeoff in three contexts: Frugality moderating privacy and security concerns. *Journal of Computer Information Systems, 55*(1), 13–29. https://doi.org/10.1080/08874417.2014.11645737.

Bansal, G., Zahedi, F. M., & Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems, 24*(6), 624–644. https://doi.org/10.1057/ejis.2014.41.

BBC (2018). *Facebook scandal' hit 87 million users'.* April 4 Retrieved fromhttps://www.bbc.com/news/technology-43649018.

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management, 54*(7), 887–901. https://doi.org/10.1016/j.im.2017.01.003.

Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly, In Press.*. https://doi.org/10.1016/j.giq.2018.04.002.

Chellappa, R. K. (2008). *Consumers' trust in electronic commerce transactions: The role of perceived privacy and perceived security. Unpublished paper.* Retrieved on July 5, 2018, fromAtlanta, GA: Emory University. http://www.bus.emory.edu/ram/papers/sec-priv.pdf.

Chen, Y., & Zahedi, F. M. (2016). Individuals' internet security perceptions and behaviors: Polycontextual contrasts between the United States and China. *MIS Quarterly, 40*(1), 205–222. https://doi.org/10.25300/misq/2016/40.1.09.

Choi, B. C., & Land, L. (2016). The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage. *Information & Management, 53*(7), 868–877. https://doi.org/10.1016/j.im.2016.02.003.

Cortina, J. M., Chen, G., & Dunlap, W. P. (2001). Testing interaction effects in LISREL: Examination and illustration of available procedures. *Organizational Research Methods, 4*(4), 324–360. https://doi.org/10.1177/109442810144002.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce–a study of italy and the united states. *European Journal of Information Systems, 15*(4), 389–402. https://doi.org/10.1057/palgrave.ejis.3000590.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems, 22*(3), 295–316. https://doi.org/10.1057/ejis.2012.23.

Dropbox (2018). *Dropbox privacy policy.* April 17 Retrieved fromhttps://www.dropbox.com/privacy.

Eastin, M. S., Brinson, N. H., Doorey, A., & Wilcox, G. (2016). Living in a big data world: Predicting mobile commerce activity through privacy concerns. *Computers in Human Behavior, 58*, 214–220. https://doi.org/10.1016/j.chb.2015.12.050.

Foldnes, N., & Hagtvet, K. A. (2014). The choice of product indicators in latent variable interaction models: Post hoc analyses. *Psychological Methods, 19*(3), 444–457. https://doi.org/10.1037/a0035728.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.2307/3151312.

Gefen, D., Straub, D., & Boudreau, M. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems, 4*(7), 1–70.

Gerlach, J., Widjaja, T., & Buxmann, P. (2015). Handle with care: How online social network providers' privacy policies impact users' information sharing behavior. *The Journal of Strategic Information Systems, 24*(1), 33–43. https://doi.org/10.1016/j.jsis.2014.09.001.

Gross, A. (2015). *Starbucks data breach shows the real damage of a breach.* May 14 Retrieved fromhttps://www.hipaasecurenow.com/index.php/starbucks-data-breach-shows-real-damage-breach/.

Hair, J. F., Jr., Anderson, R. E., Tatham, R. L., & Black, W. C. (2013). *Multivariate data analysis* (7th ed.). Pearson New International: Pearson Education Limited.

Harris, M. A., Brookshire, R., & Chin, A. G. (2016). Identifying factors influencing consumers' intent to install mobile applications. *International Journal of Information Management, 36*(3), 441–450. https://doi.org/10.1016/j.ijinfomgt.2016.02.004.

Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly, 37*(1), 275–298. https://doi.org/10.25300/misq/2013/37.1.12.

Hopwood, S. (2017). *How many mobile apps are actually used?* June 22 Retrieved fromApptentivehttps://www.apptentive.com/blog/2017/06/22/how-many-mobile-apps-are-actually-used/.

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling A Multidisciplinary Journal, 6*(1), 1–55. https://doi.org/10.1080/10705519909540118.

Jia, R., Steelman, Z. R., & Reich, B. H. (2017). Using mechanical turk data in IS research: Risks, rewards, and recommendations. *CAIS, 41*, 14.

Johnson, V. L., Kiser, A., Washington, R., & Torres, R. (2018). Limitations to the rapid adoption of M-payment services: Understanding the impact of privacy risk on M-payment services. *Computers in Human Behavior, 79*, 111–122. https://doi.org/10.1016/j.chb.2017.10.035.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549–566. https://doi.org/10.2307/25750691.

Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal, 25*(6), 637–667. https://doi.org/10.1111/isj.12082.

Keith, M. J., Babb, J., Furner, C., Abdullat, A., & Lowry, P. B. (2016). Limited information and quick decisions: Consumer privacy calculus for mobile applications. *AIS Transactions on Human-Computer Interaction, 8*(3), 88–130. https://doi.org/10.17705/1thci.00081.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-computer Studies, 71*(12), 1163–1173. https://doi.org/10.1016/j.ijhcs.2013.08.016.

Kim, D. J. (2008). Self-perception-Based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study. *Journal of Management Information Systems, 24*(4), 13–45. https://doi.org/10.2753/mis0742-1222240401.

Kim, D. J., Steinfield, C., & Lai, Y. (2008). Revisiting the role of web assurance seals in business-to-consumer electronic commerce. *Decision Support Systems, 44*(4), 1000–1015. https://doi.org/10.1016/j.dss.2007.11.007.

King, N. J., & Jessen, P. W. (2010). Profiling the mobile customer – Privacy concerns when behavioural advertisers target mobile phones – Part I. *Computer Law & Security Report, 26*(5), 455–478. https://doi.org/10.1016/j.clsr.2010.07.001.

Kumar, A. (2016). *Risk of mobile threats and privacy concerns grow.* June 3 Retrieved fromCSO onlinehttps://www.csoonline.com/article/3078815/security/risk-of-mobile-threats-and-privacy-concerns-grow.html.

Levenson, H. (2016). *7 common reasons users are abandoning your app.* August 2 Retrieved fromWeb Analytics Worldhttps://www.webanalyticsworld.net/2016/08/why-users-are-abandoning-your-mobile-app.html.

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems, 51*(3), 434–445. https://doi.org/10.1016/j.dss.2011.01.017.

Lin, G., Wen, Z., Marsh, H. W., & Lin, H. (2010). Structural equation models of latent interactions: Clarification of orthogonalizing and double-mean-centering strategies. *Structural Equation Modeling, 17*(3), 374–391. https://doi.org/10.1080/10705511.2010.488999.

Lin, Y., Huang, C., Wright, M., & Kambourakis, G. (2014). Mobile application security. *Computer, 47*(6), 21–23. https://doi.org/10.1109/MC.2014.156.

Liu, Z., & Wang, X. (2018). How to regulate individuals' privacy boundaries on social network sites: A cross-cultural comparison. *Information & Management, 55*(8), 1005–1023. https://doi.org/10.1016/j.im.2018.05.006.

Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems, 27*(4), 163–200. https://doi.org/10.2753/mis0742-1222270406.

Luo, X., Li, H., Zhang, J., & Shim, J. P. (2010). Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decision Support Systems, 49*(2), 222–234. https://doi.org/10.1016/j.dss.2010.02.008.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032.

Marsh, H. W., Wen, Z., & Hau, K. T. (2004). Structural equation models of latent interactions: Evaluation of alternative estimation strategies and indicator construction. *Psychological Methods, 9*(3), 275–300. https://doi.org/10.1037/1082-989x.9.3.275.

Mobile Ecosystem Forum (2016). *MEF global consumer trust report 2016*Retrieved fromhttps://mobileecosystemforum.com/programmes/consumer-trust/global-consumer-trust-report-2016/.

Nikkhah, H. R., & Sabherwal, R. (2017a). A privacy-security model of mobile cloud computing applications. *Proceedings of International Conference on Information Systems, 2017a*. Retrieved from https://aisel.aisnet.org/icis2017/Security/Presentations/17/.

Nikkhah, H. R., & Sabherwal, R. (2017b). Mobile cloud-computing applications: A privacy cost-benefit model. *Proceedings of Americas Conference on Information Systems*. Retrieved from https://aisel.aisnet.org/amcis 2017/InformationSystems/Nikkhah.

Nikkhah, H. R., Balapour, A., & Sabherwal, R. (2018). Mobile applications security: Role of privacy. *Proceedings of Americas Conference on Information Systems, 2018*. Retrieved from https://aisel.aisnet.org/amcis2018/Security/Presentations/18/.

Nikkhah, H. R., Grover, V., & Sabherwal, R. (2018). Why do users continue to use mobile cloud computing applications? A security-privacy investigation. *In: Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy*. Retrieved from https://www.albany.edu/wisp/papers/WISP2018_paper_30.pdf.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs, 41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x.

Okazaki, S., Li, H., & Hirose, M. (2009). Consumer privacy concerns and preference for degree of regulatory control. *Journal of Advertising, 38*(4), 63–77.

Ooi, K., & Tan, G. W. (2016). Mobile technology acceptance model: An investigation using mobile users to explore smartphone credit card. *Expert Systems with Applications, 59*, 33–46. https://doi.org/10.1016/j.eswa.2016.04.015.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research, 2*(1), 1–28. https://doi.org/10.1287/isre.2.1.1.

Osatuyi, B., Passerini, K., Ravarini, A., & Grandhi, S. A. (2018). Fool me once, shame on you … then, I learn." An examination of information disclosure in social networking sites. *Computers in Human Behavior, 83*, 73–86. https://doi.org/10.1016/j.chb.2018.01.018.

Pagliery, J. (2015). *Hackers are draining bank accounts via the Starbucks app.* May 14 Retrieved fromCNN Businesshttps://money.cnn.com/2015/05/13/technology/hackers-starbucks-app/index.html.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly, 31*(1), 105–136. https://doi.org/10.2307/25148783.

Perez, S. (2017). *Majority of U.S. Consumers still download zero apps per month, says comScore.* Retrieved from:https://techcrunch.com/2017/08/25/majority-of-u-s-consumers-still-download-zero-apps-per-month-says-comscore/.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure.* New York: Suny Press.

Petronio, S. (2008). *Communication privacy management.* Wiley Online Libraryhttps://doi.org/10.1002/9781118766804.wbiect138.

Podsakoff, M. P., MacKenzie, B. S., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *The Journal of Applied Psychology, 88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879.

Ponte, E. B., Carvajal-Trujillo, E., & Escobar-Rodríguez, T. (2015). Influence of trust and perceived value on the intention to purchase travel online: Integrating the effects of assurance on trust antecedents. *Tourism Management, 47*, 286–302. https://doi.org/10.1016/j.tourman.2014.10.009.

Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model: The case of working professionals in France and the U.K. who use online communities. *European Journal of Information Systems, 19*(2), 181–195. https://doi.org/10.1057/ejis.2010.15.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., … Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly, 37*(4), 1189–1210.

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management, 51*(5), 551–567.

Privacypolicies (2018). *Privacy policies are legally required.* November 20 Retrieved fromhttps://privacypolicies.com/blog/privacy-policies-legally-required/.

Reychav, I., Beeri, R., Balapour, A., Raban, D. R., Sabherwal, R., & Azuri, J. (2019). How reliable are self-assessments using mobile technology in healthcare? The effects of technology identity and self-efficacy. *Computers in Human Behavior, 91*, 52–61.

Roca, J. C., García, J. J., & de la Vega, J. J. (2009). The importance of perceived trust, security and privacy in online trading systems. *Information Management & Computer Security, 17*(2), 96–113. https://doi.org/10.1108/09685220910963983.

Shah, M. H., Peikari, H. R., & Yasin, N. M. (2014). The determinants of individuals' perceived e-security: Evidence from Malaysia. *International Journal of Information Management, 34*(1), 48–57. https://doi.org/10.1016/j.ijinfomgt.2013.10.001.

Shaw, N., & Sergueeva, K. (2019). The non-monetary benefits of mobile commerce: Extending UTAUT2 with perceived value. *International Journal of Information Management, 45*, 44–55. https://doi.org/10.1016/j.ijinfomgt.2018.10.024.

Shin, D. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with Computers, 22*(5), 428–438. https://doi.org/10.1016/j.intcom.2010.05.001.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1016. https://doi.org/10.2307/41409970.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167–196. https://doi.org/10.2307/249477.

Statista (2018). *Average number of new Android app releases per day from 3rd quarter 2016 to 1st quarter 2018.* Retrieved fromhttps://www.statista.com/statistics/276703/android-app-releases-worldwide/.

Straub, D., Boudreau, M., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems, 13*(1), 380–427.

Susanto, A., Chang, Y., & Ha, Y. (2016). Determinants of continuance intention to use the smartphone banking services: An extension to the expectation-confirmation model. *Industrial Management & Data Systems, 116*(3), 508–525. https://doi.org/10.1108/imds-05-2015-0195.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research, 22*(2), 254–268. https://doi.org/10.1287/isre.1090.0260.

Walton, S. C., & Rice, R. E. (2013). Mediated disclosure on Twitter: The roles of gender and identity in boundary impermeability, valence, disclosure, and stage. *Computers in Human Behavior, 29*(4), 1465–1474. https://doi.org/10.1016/j.chb.2013.01.033.

White, G., Ekin, T., & Visinescu, L. (2017). Analysis of protective behavior and security incidents for home computers. *Journal of Computer Information Systems, 57*(4), 353–363. https://doi.org/10.1080/08874417.2016.1232991.

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems, 106*, 44–52. https://doi.org/10.1016/j.dss.2017.12.003.

Wu, K., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior, 28*(3), 889–897. https://doi.org/10.1016/j.chb.2011.12.008.

Wurmser, Y. (2018). *Mobile time spent 2018: Will smartphones remain ascendant?* June 18 Retrieved fromeMarketerhttps://www.emarketer.com/content/mobile-time-spent-2018.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(12), 798–824. https://doi.org/10.17705/1jais.00281.

Xu, H., Teo, H., Tan, B. C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems, 26*(3), 135–174. https://doi.org/10.2753/mis0742-1222260305.