Intention To Disclose Personal Information Via Mobile Applications: A Privacy Calculus Perspective

By: Tien Wang, Trong Danh Duong, and **Charlie C. Chen**

Abstract

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

Wang, T., et al. (2016). "Intention to disclose personal information via mobile applications: A privacy calculus perspective." International Journal of Information Management 36(4): 531-542. https://doi.org/10.1016/j.ijinfomgt.2016.03.003. Publisher version of record available at: https://www.sciencedirect.com/science/article/pii/S0268401215300797

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

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

[a] Institute of International Management, College of Management, National Cheng Kung University, Tainan, Taiwan R.O.C. No.1, University Road, Tainan City 701, Taiwan, ROC
[c] Department of Computer Information Systems & Supply Chain Management, Appalachian State University, Boone, NC, USA, 287 Rivers St, Boone, NC 28608, USA

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

a b s t r a c t

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

1. Introduction

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

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

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

http://dx.doi.org/10.1016/j.ijinfomgt.2016.03.003

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

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

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

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

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

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

2. Conceptual foundation and research hypotheses

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

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

Customers are likely to disclose personal information via mobile devices if their perceived benefits of doing so are high. The success of these personalized mobile services heavily relies upon the collection and analysis of detailed personal information. In receiving personalized services, customers face the risk of having their personal information (e.g. location, shopping preference, medical history, and social networks) compromised as a result of the lack of security control across servers and/or client sites. Therefore, perceived benefits and risks must be considered at the same time to understand the decision of users to disclose personal information via mobile devices.

Previous studies have identified several factors that affect the perception of risks based on privacy calculus theory. For example, Li (2012) conducted a literature review and listed the factors that can discourage and encourage personal information disclosure. The review suggests that the majority of the studies on this topic examine risks and benefits separately and that only a few studies have analyzed the relative influence of privacy concern on the intention of personal information disclosure in an e-commerce context (Dinev & Hart, 2003, 2006). This study attempts to fill the research gap by suggesting a balanced approach for examining both the relative and joint benefits and risks of disclosing personal information via mobile apps.

2.1. *Investigating the antecedents of trade-off analysis through the calculus lens*

According to privacy calculus theory, consumers conduct a risk–benefit analysis when deciding to disclose personal informa- tion in a digital context. Given that most users are cognizant of the dangers of disclosing personal information without sufficient assurance, the risk–benefit assessment is becoming a common practice in the digital world (Milne, Rohm, & Bahl, 2004). Before allowing firms to access their privacy information, customers often examine the potential benefits and risks they receive and encounter. The privacy issue is more critical in the mobile context because a variety of personal information, such as exact time, location, and preference relevant to a specific behavior, is readily available the minute customers agree to provide such information via mobile apps. In addition, an increasing number of users access online services and contents through mobile devices instead of through a landline connection. In this case, increasing consumers' intention to disclose their personal data through a mobile platform becomes important to marketers with regard to consumer data collection. This study proposes two driving forces of perceived benefits derived from the provision of personal information and the other two additional factors of perceived risk incurred due to personal information revelation.

The first driving force of perceived benefits is self-presentation. Self-presentation refers to the behavior of consumers to intentionally regulate their personal image in the eyes of others. In the Web 2.0 environment, users may display, edit, and manage their own information for self-presentation such as online personal brands (Labrecque, Markos, & Milne, 2011). The personal information arranged for others to see may include demographic profiles, photos, selfies, videos, and friends lists (Lee, Ahn, & Kim, 2014). These digital materials may provide more social cues than those revealed by body language, a type of expression that can hardly be detected in non-face-to-face communications. For example, the functions on Facebook, including check-in, like, comment, and share, allow users to express and manage their identity and image (Lee et al., 2014). When using the "check-in" function of mobile Facebook, users can disclose their whereabouts at a specific time. People can also "tag" their friends in real-time. These expressions, coupled with location-based data at a specific time not only provide other people with information on an individual's social network connections, but also allow others to match what they say with what they do. The combined temporal and spatial information further completes a person's online profile. Self-presentation can be translated into a form of communication behavior that motivates individuals to disclose or share self-provided information, helping them construct and maintain their public self-image (Lee-Won, Shim, Joo, & Park, 2014; Rui & Stefanone, 2013). Individuals can realize the behavior of expressing their self-presentation on mobile devices by pressing a "Like" button, changing individual social status, sharing a comment, or posting a picture, a video, or an emoticon or by "checking-in" to show their locations and tagging their friends. These interaction mechanisms can be used as self-presentation tools because customers can use them to intentionally disclose personal information via mobile apps and construct and maintain their public self-images. Based on the preceding discussion, we propose the following hypothesis:

H1. Self-presentation behavior is positively related to the perceived benefits of personal information disclosure via mobile applications.

The second driving force, personalization, requires collecting and using personal information to tailor services and contents to target customers. Consumers are generally willing to reveal their personal information to receive personalized services, including birthday coupons and recommended books (Li, 2014; Taylor, Davis, & Jillapalli, 2009). A survey shows that customers often welcome personalized services, such as offering an ad in exchange for a specific product for which they have been looking (Lee, 2014). These personalized cues of immediacy can increase the intentions of users to disclose embarrassing and descriptive information (Bandura, 1986; Lee & LaRose, 2011).

When consumers disclose personal information to firms in the mobile context, the latter may collect and analyze the data and subsequently design customized services for the former. If customers allow marketers to collect their location data, then the firms can provide a specific promotion package that is only available at an exact time and location. For instance, most mobile users are encouraged to share their phone number and location information to redeem an attractive offer (e.g., "check-in with store logo and receive 10% discount"). Such a promotion can also be tailored to individual preference if substantial consumption data are available to firms (Davenport, Mule, & Lucker 2011). In return, customers may gain monetary rewards, discounts, and convenience, or save time. Mobile technologies (e.g., wearables and mobile devices) can instantly be connected with one another via the IoT platform, which changes not only how people live but how they shop as well. When customers allow marketers to access their mobile information, the services can be personalized to a sophisticated level and deeply immersed into the formers' daily lives. The scope and depth of personalized services are expanded in the mobile environment and thus greatly benefit customers. For instance, tourist recommendation systems emerge from the effective use of mobile devices to obtain customer profiles and site preferences and consequently make recommendations about points of interest to improve trip experiences (Anacleto, Figueiredo, Almeida, & Novais, 2014). Conversely, customers cannot enjoy personalized services and related benefits if they do not disclose their useful personal information to mobile service providers. Therefore, the following hypothesis is drawn:

H2. Personalized services are positively related to the perceived benefits of personal information disclosure via mobile applications.

For perceived risks, this study proposes and examines two other driving factors, namely, perceived severity and control. Perceived severity refers to the manner in which individuals perceive the negative consequences due to a security threat, which triggers their

privacy protection behaviors (LaRose, Rifon, Liu, & Lee, 2005). Perceived severity is significantly related to protective and avoidance behaviors, such as enabling the security measures of a wireless home network and installing an anti-malware software (Lee & Larsen, 2009). The individuals who perceive severe consequences as a result of losing information privacy tend to become highly concerned about their information security (Mohamed & Ahmad, 2012) and undertake the required action to protect their personal data. Such concern can even become intensified in the mobile context in which the people, objects, and things are closely and tightly connected. Thus, this research hypothesizes that the consumers who perceive severe consequences experience high perceived risks when they disclose their personal information via mobile apps.

H3. The perceived severity of personal information disclosure via mobile applications is positively related to consumers' perceived risks.

Withholding information from being disclosed allows consumers to control their submitted personal information to offset the risk of possible negative issues (Dinev & Hart, 2004). In the literature, control allows consumers to decide how much information to disclose, how they like others to perceive them, or how they should disclose themselves (Derlega & Chaikin, 1977; Stone & Stone, 1990). Various uses of information control can reduce the privacy concerns of consumers over the invasion of their privacy (Laufer & Wolfe, 1977). When consumers feel that they have control over future personal information and how it will be used, they feel a reduced sense of having been invaded or become less concerned about the risks of losing their information privacy (Culnan & Armstrong, 1999). Firms can provide their customers with multiple means (e.g., opt-out, privacy notices, and consent forms) to control their personal information in the mobile context. However, for strategic and managerial reasons, firms may also limit such functions (e.g., temporary opt-out instead of permanent opt-out) (Labrecque et al., 2011). If the firm offers a high level of control, then consumers can be less concerned about the risks of their personal information being compromised (Malhotra, Kim, & Agarwal, 2004).

H4. Perceived control of personal information disclosure via mobile applications is negatively related to customers' perceived risks

2.2. *Understanding the outcomes of privacy calculus*

Privacy calculus theory asserts that when consumers allow product or service providers to access their personal information, they will perform the costs (risks)–benefits analysis of motivational factors that enable and inhibit information disclosure (Awad & Krishnan, 2006). If the consumers feel that they can gain benefits, such as convenience (Milne & Gordon, 1993), customized and personalized services (Awad & Krishnan, 2006; Graeff & Harmon, 2002; Xu et al., 2011), entertainment (Lee, Im, & Taylor, 2008), and personal image and monetary rewards (Lee et al., 2008), from disclosing personal information, then they will generally relinquish some level of their privacy for potential benefits while using mobile phone apps.

H5. Perceived benefits are positively related to the intention to disclose personal information via mobile applications

Perceived risks pertain to the problems that may occur for customers when firms have access to their personal information (Malhotra et al., 2004). The ethical use of privacy data to which firms have been granted access is uncertain. Customers have concerns that unethical firms may access other privacy data they have not been permitted to retrieve. Customers also worry that their privacy data may be sold to a third party without prior notice or consent (Xu et al., 2011). Following this line of reasoning, we posit that the overall risk perception of information disclosure is expected to negatively affect consumers' intentions to disclose their information to a marketer (Norberg, Horne, & Horne, 2007). As such, the intention of consumers to disclose their personal information will decrease if they identify a high risk of privacy invasion while using mobile phone apps.

H6. Perceived risks are negatively related to the intention to disclose personal information via mobile applications.

Considering the effects of benefits and risks, our research framework will examine the conflicting forces in the mobile environment in which the diverging effects coexist and the boundary is blurred. We will also investigate the relative strength of the different relationships in the model and obtain further knowledge on user behavior in the mobile environment.

3. Methodology

3.1. *Questionnaire design and measurement items*

An online survey was employed to collect data for hypothesis testing and the respondents were invited through paid advertising on online portals and researcher networks. To reach out to potential qualified respondents, a paid campaign was run for two weeks on Facebook. The targeted subjects were individuals aged 16 years and above with keen interest in mobile apps, social media, social networking, etc. Upon logging in, the ad recipients were exposed to the research information via their Facebook page. The research information was also posted on the university's student networks and on the personal fan pages of the researchers to recruit other potential respondents.

The questionnaire was comprised of three parts. The first section explained the purpose and context of the research. In the second section, the respondents were instructed to provide their opinions about all of the measurement items. An attempt was made to counterbalance the sequence of questions of different constructs to create a psychological break and to avoid respondent fatigue (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). Finally, the third section contained demographic questions. Confidentiality and anonymity of all respondents were maintained.

The research model incorporated seven constructs, namely, self-presentation, personalized services, perceived severity, perceived control, perceived benefits, perceived risks, and intention to disclose via mobile apps. All questionnaire items were adapted from the existing literature to fit the current research context and were assessed with a seven-point Likert scale ranging from 1 ("strongly disagree") to 7 (strongly agree"). Table 1 presents the summary of measurement items.

The control variables included demographic information, such as gender and education. Previous studies indicated that prior experiences of mobile app usage can influence the intention of personal information disclosure (Bansal, Zahedi, & Gefen 2010; Kim, Ferrin, & Rao, 2008). To avoid the potential influence of prior experiences, we added three control variables, namely, years of smartphone ownership, number of hours spent on mobile app usage every week, and number of apps used every week.

3.2. *Characteristics of the sample*

A total of 347 survey questionnaires were collected and 327 were retained for further analyses after data cleaning. Table 2 lists the demographics and characteristics of the smartphone usage of the respondents. Approximately 81.3% of the respondents were aged 21–30 years, representing the major segment of smartphone

Table 1
Measurement items.

Construct	Items	Descriptions
Perceived severity (adapted from Mohamed & Ahmad, 2012)	SEVE1	I believe that losing information privacy through mobile applications would be a serious problem for me
	SEVE2	Having my online identity stolen through mobile applications would be a serious problem for me
	SEVE3	Losing personal information privacy through mobile applications would be a critical issue for me
	SEVE4	Losing photo privacy through mobile applications would be a serious problem for me
Perceived control (adapted from Hong & Thong, 2013)	CTRL1	I am usually bothered when I do not have control over personal information that I provide to mobile applications
	CTRL2	I am usually bothered when I do not have control or autonomy over decisions about how my personal information is collected, used, and shared by mobile applications
	CTRL3	I am concerned when personal information control is lost or unwillingly reduced as a result of a marketing transaction with mobile applications
Self-presentation (adapted from Lee et al., 2008)	SP1	I disclose to present myself in a realistic manner
	SP2	I disclose to present my self-concept
	SP3	I disclose to present my individual characteristics
Personalized services (adapted from Xu et al., 2011)	PER1	Mobile applications can provide me with personalized deals/ads tailored to my activity context
	PER2	Mobile applications can provide me with more relevant promotional information tailored to my preferences or personal interests
	PER3	Mobile applications can provide me with the type of deals/ads that I might like
Perceived benefits (adapted from Xu et al., 2011)	BEN1	Mobile applications reduce my searching time to find promotional information that I need
	BEN2	Mobile applications can provide me with the convenience to instantly access the promotional information that I need
	BEN3	Overall, I feel that using mobile applications is beneficial
Perceived risks (adapted from Xu et al., 2011)	RISK1	Providing the mobile applications with my personal information would involve many unexpected problems
	RISK2	Disclosing my personal information to mobile applications would be risky
	RISK3	The potential for loss in disclosing my personal information to mobile applications would be high
Intention to disclose via mobile applications (adapted from Xu et al., 2011)	INT1	I am likely to disclose my personal information
	INT2	I am willing to disclose my personal information
	INT3	Disclosing my personal information to this application for its product and services is unlikely for me (reverse code)

users. With regard to smartphone ownership, 12.5% of the respondents have used smartphones for less than a year, 25.1% from 1 to 2 years, 19.6% from 2 to 3 years, and 42.8% for more than 3 years. Regarding the average time spent on mobile apps, more than half of the respondents (50.8%) had spent 1 h to 20 h for the previous week, 25.7% spent 21 h to 40 h, 9.2% from 41 h to 60 h, 4.9% from 61 h to 80 h, and 3.4% spent more than 100 h. Finally, 86.2% of the respondents said that they use an average of 1–10 apps every week.

3.3. *Confirmatory factor analysis*

This study employed partial least squares (PLS; Ringle, Wende, & Will, 2005), a second-generation statistical technique, to test the measurement model. Compared with covariance-based structural equation modeling (CB-SEM), PLS is a variance-based SEM and explains the variance in dependent variables. In addition, PLS is more liberal on sample size and data distribution requirements than CB-SEM (Chin & Newsted, 1999).

Among all the measurement items, one item of perceived severity (SEVE3) and another item of intention (INT3) were removed because of low loading and high variance inflation factor (VIF) values. Kock & Lynn (2012) specified that a VIF value threshold at 3.3 is recommended within the context of variance-based SEM, such as our research.

Several assessments were conducted to ensure the convergent and discriminant validities. The average variance extracted (AVE) and composite reliabilities (CR) were first examined for convergent validity. As indicated in Table 3, all constructs had CR values greater than 0.8, exhibiting a satisfactory internal consistency. The results also showed that the AVE values ranged from 0.649 to 0.828, which were higher than the recommended level of 0.5 (Fornell & Larker, 1981). This finding suggests that more than half of the variances of the constructs were explained by the items; hence, all constructs exhibited an acceptable convergent validity.

To examine the discriminant validity, the square roots of AVE values were compared with inter-construct correlations (Fornell & Larcker, 1981). Table 3 shows that the values on the diagonals are greater than those of off-diagonals. Table 4 reports the cross-factor loadings and reveals that all items have loadings greater than 0.7 and load substantially higher on their corresponding factors. Therefore, the measurement items exhibited a satisfactory discriminant validity.

3.4. *Common method bias (CMB)*

Harman's one-factor test (Harman, 1976) was also conducted to address the common method bias (CMB) that is commonly associated with the survey approach. The following two criteria are widely adopted to determine the aspects in which the data are likely to suffer from CMB: (1) a single factor emerges from the factor analysis, and (2) one general factor accounts for the majority of the covariance among measures (Podsakoff et al., 2003). If none of these cases materializes, then the likelihood of CMB occurrence is low. The result of the unrotated principal component factor analysis showed that the first factor explained approximately 32% of the total variances. As a result, CMB was not considered a serious problem because more than one factor was extracted, and no single

Table 2
Characteristics of the sample.

Demographics	Categories	Frequency	Percentage (%)
Age	Under 20	17	5.2
	21–30	266	81.3
	31–40	35	10.7
	41–50	8	2.4
	51–60	1	0.3
Gender	Male	154	47.1
	Female	173	52.9
Education	High school or below	12	3.7
	Bachelor's degree	154	47.1
	Master's degree	148	45.3
	Doctoral degree	13	4.0
Income	Less than USD 500	178	54.4
	USD 500–1000	92	28.1
	USD 1001–2000	44	13.5
	USD 2001–3000	7	2.1
	Above 3000	6	1.8
Employment Status	Student	147	45.0
	Part-time employed	18	5.5
	Full-time employed	142	43.4
	Unemployed	7	2.1
	Others	13	4.0
Working experience (years)	None	46	14.1
	1–5	224	68.5
	6–10	45	13.8
	Above 10	12	3.7
Smartphone ownership	Less than 12 months	41	12.5
	12–24 months	82	25.1
	25–36 months	64	19.6
	More than 3 years	140	42.8
Average time spent using mobile applications last week by users (hours)	None	4	1.2
	1–20	166	50.8
	21–40	84	25.7
	41–60	30	9.2
	61–80	16	4.9
	81–100	16	4.9
	Above 100	11	3.4
Number of mobile app used weekly on average	None	4	1.2
	1–10	282	86.2
	11–20	32	9.8
	21–30	5	1.5
	Above 30	4	1.2

Table 3
Construct reliability, validity, and correlations.

	Mean	Sd	AVE	C.R.	1.	2.	3.	4.	5.	6.	7.
1. Benefits	5.019	1.193	0.649	0.846	**0.805**						
2. Control	5.134	1.333	0.796	0.921	0.497	**0.892**					
3. Intention	3.274	1.562	0.760	0.863	0.223	0.040	**0.872**				
4. Risk	5.366	1.406	0.770	0.909	0.356	0.546	−0.136	**0.877**			
5. Severity	5.732	1.326	0.775	0.912	0.432	0.654	−0.106	0.662	**0.880**		
6. Personalized services	4.851	1.206	0.739	0.894	0.579	0.447	0.074	0.316	0.437	**0.860**	
7. Self-presentation	4.241	1.485	0.828	0.935	0.273	0.151	0.360	0.075	0.116	0.264	**0.910**

*The square roots of AVEs are on the diagonal.
*1: Benefits; 2: Control; 3. Intention; 4. Risk; 5. Severity; 6. Personalized services; 7. Self-presentation.

factor accounted for more than 50% of the variances (Podsakoff & Organ, 1986).

The approach of Liang, Saraf, Hu, and Xue, 2007 was also applied to examine CMB. A method factor was introduced into the research model. The likelihood of CMB being a major concern is supported by the significant method factor loadings and the substantial values of the squared loadings. Our analysis revealed that most of the method factor loadings were insignificant, except for those between the method factor and INT1, INT2, BEN3, PER3, and SEVE1. Next, we examined the loadings and found that the squared loadings of the substantive constructs exceeded their method variances. Therefore, the likelihood of CMB occurring in this study is low. To further enhance our confidence in ruling out CMB, we employed a marker variable approach in creating a method factor (Lin, Huang, & Hsu, 2015; Rönkkö & Ylitalo, 2011). Specifically, we selected the following six items of need for cognition (NFC) collected in the survey: (1) "In general, I prefer complex to simple problems," (2) "I would prefer a task that is intellectual, difficult, and important to one that is somewhat important but does not require much thought," (3) "I find little satisfaction in deliberating hard and for long hours," (4) "I prefer to think about small, daily projects rather than long-term ones," (5) "I think primarily because I have to," and (6) "I tend

Table 4
Cross-loading values of research constructs.

	Benefits	Control	Intention to disclose	Personalized services	Risk	Severity	Self-presentation
BEN1	**0.702**	0.374	0.213	0.342	0.185	0.192	0.159
BEN2	**0.872**	0.390	0.140	0.555	0.308	0.379	0.220
BEN3	**0.832**	0.441	0.201	0.476	0.349	0.440	0.271
CTRL1	0.460	**0.888**	0.078	0.380	0.473	0.570	0.126
CTRL2	0.422	**0.921**	0.020	0.389	0.482	0.591	0.103
CTRL3	0.447	**0.867**	0.011	0.426	0.505	0.590	0.174
INT1	0.217	0.179	**0.819**	0.117	0.046	0.046	0.247
INT2	0.182	−0.061	**0.922**	0.030	−0.232	−0.188	0.365
PER1	0.493	0.449	0.035	**0.800**	0.284	0.395	0.170
PER2	0.488	0.416	0.050	**0.897**	0.297	0.389	0.237
PER3	0.508	0.290	0.104	**0.878**	0.233	0.342	0.272
RISK1	0.323	0.453	−0.113	0.272	**0.876**	0.566	0.087
RISK2	0.346	0.521	−0.095	0.298	**0.878**	0.591	0.072
RISK3	0.269	0.462	−0.150	0.260	**0.877**	0.586	0.039
SEVE1	0.401	0.653	−0.113	0.426	0.616	**0.887**	0.091
SEVE2	0.376	0.560	−0.088	0.328	0.588	**0.895**	0.099
SEVE4	0.361	0.508	−0.077	0.398	0.542	**0.860**	0.118
SP1	0.298	0.138	0.356	0.268	0.079	0.094	**0.921**
SP2	0.234	0.133	0.303	0.234	0.046	0.118	**0.916**
SP3	0.189	0.145	0.317	0.207	0.078	0.108	**0.892**

to set goals that can be accomplished only by extending considerable mental effort." These items were used to create a method factor that had a regression path to each endogenous construct as an exogenous construct. We then estimated the models with and without the method factor. Analysis results showed that the significant paths detected in the original baseline model remained significant in the method factor model. Therefore, we conclude that CMB is not a major concern in this study.

3.5. *Assessment of the structural model*

The quality of our structural model was evaluated based on R-squares. Structural paths were assessed to test the relationships of the research hypotheses. The R-squared values for the dependent variables indicate the percentage of variance in the dependent variable explained. Fig. 1 reports the analysis results of the research model. As can be seen, the perceived benefits were significantly influenced by two factors: personalized services ($\beta = 0.544$, $p \leq 0.001$) and self-presentation ($\beta = 0.129$, $p < 0.01$), which explained 35% of the variance in perceived benefits. Accordingly, H1 and H2 are supported.

For perceived risks, perceived severity and perceived control jointly explained 46.1% of the variance. Perceived severity substantially affected perceived risks in a positive manner ($\beta = 0.534$, $p < 0.01$), thereby supporting H3. In addition, perceived control significantly affected perceived risks ($\beta = 0.196$, $p < 0.01$). However, such an effect is positive, contrary to our expectation. Therefore, H4 is not supported.

Meanwhile, H5 represents a hypothetical statement indicating that perceived benefits are positively related to the intention of disclosing personal information via mobile apps. Based on the statistical results ($\beta = 0.323$, $p \leq 0.001$), the positive influence of perceived benefits on the intention of information disclosure via mobile apps is verified. Thus, H5 is supported. As for H6, it posited the idea that perceived risks are negatively related to the intention of information disclosure via mobile apps. The results indicated a negative relationship (with $\beta = -0.254$, $p \leq 0.001$) between two constructs. Thus, perceived risks are considered to be negatively related to the intention of information disclosure via mobile apps, thereby supporting H6.

We also incorporate demographic and usage variables as control variables. The results reveal that only gender and usage hours per week exert significant impacts. All other variables, including age, income and smartphone ownership, fail to influence users' intention to disclose. In other words, the introduction of control variables retained the original relationships between the antecedent and outcome variables. Therefore, we removed insignificant control variables and only retained the influential ones. Interestingly, the data suggested that consumers who spent more time using apps are less likely to disclose their personal information via apps (with $\beta = -0.147$, $p \leq 0.001$). Moreover, females are more likely to disclose personal information through mobile apps (with $\beta = 0.116$, $p \leq 0.001$).

4. Discussion

4.1. *Research findings*

The personalization–privacy paradox has long been argued as the root of the slow acceptance of some mobile technologies among consumers (Xu et al., 2011). However, this paradox has become less enduring than it used to be. A study shows that privacy issues, regardless of their safety, do not stop users from using personalized mobile applications for gratification purposes (Sutanto et al., 2013). As a result of the eroding importance of privacy concerns in adopting mobile applications, the current literature emphasizes the investigation of (1) the factors contributing to the amount of personal information that mobile users are willing to share (Han, Min, & Lee, 2015) and (2) context-aware services that can be delivered on the basis of the massive amount of personal information (Gronli, Ghinea, & Bygstad, 2013). Understanding information disclosure factors can provide insights into the design of context-aware mobile applications that would encourage users to disclose personal information (positive and negative). Consequently, mobile companionship can be achieved with the introduction of personalized, adaptive, and gratifying applications (Gronli et al., 2013).

We conceptualized a dual-path research model based on privacy calculus theory to understand the cost–benefit analysis carried out by individuals as they make decisions regarding their privacy. We posited two driving forces of each path that influence a person's intention to disclose personal information via mobile apps. Compared with perceived risks, the benefits that customers think they will receive after disclosing personal information exert a stronger influence (the absolute value of 0.323 is greater than that of −0.254) on mobile users' intention to disclose personal information. This result suggests that when using mobile apps, individuals assign greater value to potential rewards than to potential risks. This major finding matches that of a recent study about young

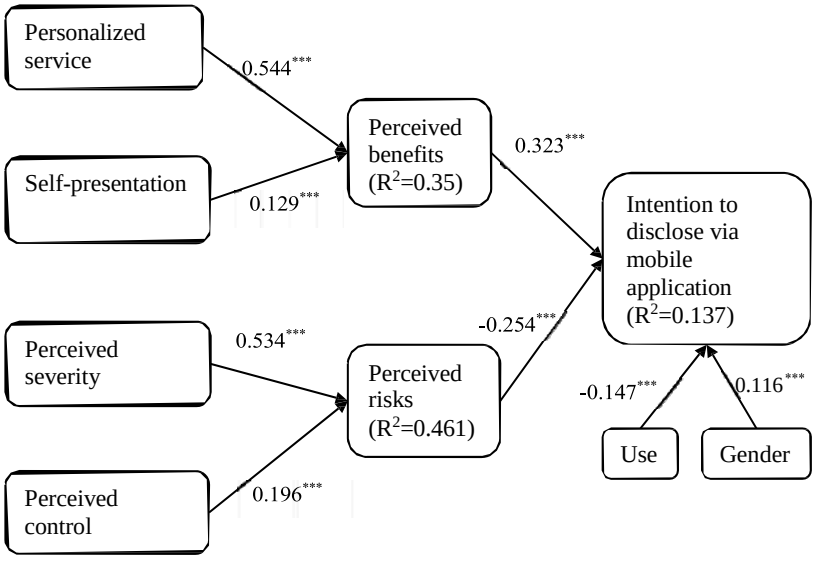

Fig. 1. Results of the research model.

Facebook users' lack of privacy concerns (perceived risks) when sharing their location-related information via mobile phones (Kim, 2016). Another study supporting our finding revealed that compared with non-mobile users, the mobile users of Twitter place greater value on the benefits of immediacy and intimacy to fulfill their social interaction needs (Han et al. 2015). Hence, when using mobile apps, an increasing number of users are placing greater importance on perceived benefits than on perceived risks.

Driving forces exert different effects in terms of magnitude. For perceived benefits, the influence of personalized services is four times greater than that of self-presentation (0.544 versus 0.129). Personalized services are social cues that can help users form trust in the mobile services they receive. A high degree of personalized immediacy services can encourage mobile users to disclose both descriptive and even embarrassing information (e.g., personal health records) about themselves (Lee & LaRose, 2011).

In addition, enabling users to establish symbolic self-representation can also encourage users to disclose their personal information in mobile applications. Self-representation portrays shared network experiences and a common understanding of individual roles (Byron & Laurence, 2015). To develop, maintain, and improve their personal relationships in mobile applications, users feel inclined to share personal information. Mobile applications that contribute to self-regulation behaviors can attract a large number of users who are willing to share their personal information over such mobile apps. One major reason for the ubiquitous acceptance of YouTube is its ability to encourage video creators to visually disclose personal information in non-anonymous settings (Misoch, 2015).

Although the security risks of mobile commerce are omnipresent in today's society, mobile users tend to have relatively low perceived risks (Jones & Chin, 2015). Perceived risks have been proven to be an important predictor for Internet technology (e.g., e-banking) adoption in previous studies (Martins, Oliveira, & Popovic, 2014). Our study suggests the close examination of the two antecedents of perceived risks, namely, perceived severity and perceived control. Our findings show that perceived benefits have the same pattern as perceived risks. Specifically, perceived severity exerts a stronger influence on perceived risks relative to perceived control. The influence of perceived severity (path coeffi- cient = 0.534) is almost three times greater than that of perceived control (path coefficient = 0.196). The finding is consistent with that of previous studies, which reported that perceived severity (e.g., service failure severity and product performance risks) has a strong negative influence on customer metrics such as loyalty (Wang, Wu, Lin, & Wang, 2011) and trust (Hong, 2015). Security risk and perceived risks are not increasing at the same rate, thus highlighting the importance of increasing users' perceived risks to the same level as security risks. For instance, most users are not aware of the potential and prevalent risks (e.g., information security, data location, provider lock-in, and disaster recovery) inherent in cloud computing applications (Brender & Markov, 2013). To heighten users' awareness of the perceived risks of using mobile applications on the cloud, communicating with them about the severity of losing their personal data on the cloud could be more effective than educating them about not disclosing their sensitive, personal data.

Although the empirical data generally support most of the hypotheses, we still obtained an unexpected result that is inconsistent with our proposed hypothesis. We proposed a negative effect of perceived control on perceived risks, whereas the analysis revealed the possibility that a high level of perceived control actually activates customers' awareness on the probability of privacy invasion. A possible explanation is that a person who scores high in terms of self-control of perceived risks is likely to be strongly aware of or sensitive to privacy threats. This positive relationship is particularly evident among mobile users. The Pew Research Center conducted a survey with 88% of adult mobile phone owners and users and found that smartphone users are especially vigilant about how personal data in their mobile devices would be used (Boyles, Smith, & Madden, 2012). About 54% of the mobile users in the study chose not to install certain apps after learning potential risks of information disclosure via such apps. Another 30% of the mobile users in the study exerted extra efforts to uninstall apps that posed privacy risks. Furthermore, about 60%, 50%, and 30% of mobile users backup content, clear browsing history, and turn off location tracking features in their smart phones, respectively. Evidence from the study affirms that the negative relationship between self-control and perceived risks often seen in the wired environment is no longer applicable to the mobile environment.

4.2. *Additional analysis on boundary conditions*

In order to enhance our understanding of users' intention to disclose via mobile apps, we have examined possible bound- ary conditions with variables we collected. We test whether any

demographic variable (e.g., gender, age, education, income and the duration of smartphone ownership) is able to strengthen or weaken any hypothesized relationship in the research model. The results show that all variables have neither direct nor moderating effect on the outcome variable, except gender. Although females tend to disclose more personal information via mobile apps, gender does not change, strengthen, or weaken the hypothesized relationships.

5. Conclusion

5.1. Theoretical contributions

This research offers theoretical contributions in several aspects. First, the findings of this study suggest that, in addition to technical attributes, consumers' perceptions significantly influence their decision to disclose personal information. To this end, this research expands prior studies by incorporating non-technical and more psychological factors into the privacy calculus (Dinev & Hart 2003) and provides a novel perspective for examining the personalization–privacy paradox in the mobile context.

Second, this study differs from previous studies because of its use of the privacy calculus model to examine users' intention to disclose personal information in the process of adopting mobile services. The current literature often measures perceived benefits and risks with more emphasis on one over the other (Dinev & Hart 2003) and the overall value of information disclosure (Morosan & DeFranco, 2015), or extends the privacy calculus model by integrating other variables, such as gender (Sun, Wang, Shen, & Zhang, 2015), various intervention mechanisms (Xu et al., 2009), potential information recipients (James, Warkentin & Collignon, 2015), and culture (Krasnova, Veltri, & Gunther, 2012). By contrast, this study closely examines perceived benefits and risks by assessing them and their antecedents simultaneously through dual paths in the mobile context.

Third, this work extends the previous work on the privacy calculus model (Dinev & Hart 2003; Xu et al., 2011) by identifying four driving forces, namely, two driving forces for perceived benefits and two driving forces for perceived risks, which contribute to the ultimate disclosure of personal information. Specifically, personalized services and self-presentation increase consumer perception of the benefits of sharing information with mobile app service providers, whereas perceived severity and perceived control enhance consumer awareness of the risks of information disclosure. The empirical analysis supports these two paths of the influence of perceived benefits and risks on disclosure intention, thus presenting a balanced framework based on privacy calculus theory.

Fourth, our findings offer novel insights into the differential effects of perceived benefits and perceived risks on personal information disclosure via mobile applications. As users become less concerned with or aware of privacy protection in the mobile context, they tend to emphasize trade-off values. In addition, when seeking personal benefits, mobile users tend to consider personalized services as having higher value than self-representation. In encouraging mobile users to share their personal information, lowering the perceived severity of losing their personal information is more effective than equipping them with stringent security control. These differential effects were not established in previous studies.

Fifth, the positive relationship between perceived control and perceived risks contradicts our expectation and suggests a research avenue, in which the effect of this factor may be hypothesized to be dependent on context. Xu et al. (2011) argued that privacy decision-making is contextual in nature and reported that mobile users' risk perception is relatively strong when the personalization approach is proactive-based. Therefore, such a result extends the literature on privacy calculus through the additional empirical evidence of contextual factors.

5.2. Managerial implications

This study also offers practical insights for businesses that attempt to provide customers with access to their services through mobile avenues. The findings suggest that customers value benefits more than they do risks. In other words, customers place more weight on benefits than on risks. Businesses should take advantage of this knowledge and subsequently shape their value propositions to customers. Given that customers are willing to take some risks to receive certain hedonic and utilitarian benefits, mobile service providers should exert additional efforts to make the benefits salient and distinct through effective promotional plans. In doing so, these providers can further entice customers to take the risk of releasing personal information and enjoying personalized services.

One approach is to offer dynamic user experiences based on personalized information, because such services can create a win–win situation for both providers and mobile users. The first step toward offering a gratifying experience is for a business to successfully convince its users to disclose personal information. Our study suggests that efforts should be first spent on customizing the current mobile service offerings for users, followed by helping them create a symbolic identity. With such efforts, users may be willing to disclose their personal information and help mobile application developers further enhance the offerings of their current personalized mobile services. More importantly, users within the same symbolic social network will grow steadily and become a profitable market segment.

Meanwhile, mobile service providers should strive to minimize the perceived failure severity of having users' personal information compromised. If users sense a high perceived severity of their personal information being abused by mobile service providers, they will be less likely to disclose it. Furthermore, mobile service providers can provide users with added degree of control so that they can decide what, with whom, and how their personal information should be shared and disseminated in their mobile network.

Information technology enables firms to collect a large amount of customer data. Firms with a superior capacity to analyze big data and design particular products or services tailored to customer needs are likely to obtain their customers' permission to access their personal data. To deliver personalized mobile services, a growing number of companies are currently utilizing social media analytics techniques, such as opinion mining, sentiment analysis, social network analysis, and visual analytics. The key to the success of these strategies is treating social network users as co-creators of their personalized products or services (Fan & Gordon, 2014). Failing to encourage users to disclose personal information can lead to the failure of even the most cutting-edge business analytics technologies.

Our research also provides guidelines that shall serve as bases for firms' implementation of their respective segmentation and targeting strategies. The self-presentation in our study assesses people's tendencies to reveal themselves in the eyes of others and represents an important personality feature. In marketing, the variables that capture consumers' personality features and lifestyles represent essential components of psychographics, which are commonly used for market segmentation and targeting. For instance, a previous study reported that mobile phone users can be grouped into three mobile lifestyles or segments—trendy users, engaged users, and thrifty users—based on their attitude toward using mobile phone as a self-presentation article for fashion (Vanden, Antheunis, & Schouten, 2014). In addition, some prior studies indicated that motivational factors drive the extent to which mobile users are willing to reveal personal information online (Hsiao,

Chang & Tang, 2016; Lee & Kwon, 2015). Therefore, we suggest that firms should use this psychographic as a segmentation basis to target customers who have a high motivation to reveal and shape their digital identity with mobile devices. Mobile technologies provide numerous tools and avenues for creating and spreading personalized digital artifacts. These digital materials not only enable the self-extension of a user, but also serve as the extended-self of such user for others to know (Belk, 2013). Companies can then segment their customers according to the motivational factors of disclosing personal information in mobile applications. Moreover, firms should consider avoiding users who are sensitive to risks. For example, considering one of our interesting findings that females have a greater tendency than males to disclose their personal information via mobile apps, firms may thus consider females who are insensitive to technological issues as a priority market segment.

5.3. *Limitations and future research*

Although our study documents the importance of perceptual factors in disclosing information among mobile app users, we are unable to test all of them in one research model. Hence, researchers are encouraged to build upon our study and explore other potential psychological factors. In addition, our finding of the positive influence of perceived control on perceived risks suggests the possibility of moderators. Hence, another future research opportunity would be to examine the contextual factors that may alter the relationships tested in this work. For example, Xu et al. (2011) reported that the personalization–privacy paradox depends on personalization approaches (e.g., covert versus overt, for location-aware marketing). In an additional attempt, we tested our method factor, need for cognition (NFC), as a potential moderator because it assesses users' motivation to process information cognitively. Prior literature on communication and information processing suggests that the level of users' need for cognition influences Internet use behavior (Amichai-Hamburger, Kaynar, & Fine, 2007). Thus, assuming that people with different levels of need for cognition may act as a boundary condition to alter the relationships is reasonable. Our preliminary analysis showed that the moderation effect of NFC on the relationship between risk and disclosure (Risk * NFC) is significant and negative, whereas that for benefit is insignificant. As the initial attempt of this study is to test the common method bias issue of this study, we only used a partial set of items in our survey to avoid respondent fatigue. Future research efforts could investigate these potential factors, which may change the magnitude or direction of the effects on the intention to disclose personal information in the mobile context.

Users embrace the use of mobile apps to enjoy personalized services and promote their identity and public image. However, a growing number of users have privacy concerns (Milne et al., 2004) because some mobile app providers utilize personal information unethically. Thus, these users perceive the risk of personal information disclosure and often attempt to exercise some control when using mobile apps. For instance, reading the privacy policy can reduce the risks of disclosing personal information and promote choices (Milne & Culnan, 2004) for mobile users.

This exploratory study adopts the privacy calculus model to examine the trade-off decision made by users before disclosing personal information via mobile apps. The results indicate that perceived benefits has greater influence than perceived costs on the decision of mobile users to disclose personal information via mobile apps. To increase the perceived benefits, mobile app providers should thus emphasize the provision of customized services and help users manage their identities. Moreover, application providers should reduce the degree of perceived severity to encourage users to disclose their personal information. Understanding the personalization/privacy paradox can aid mobile app providers in offering more personalized and privacy-aware products and services. Consequently, a win–win situation can be created for both users and mobile app providers.

References

Amichai-Hamburger, Y., Kaynar, O., & Fine, A. (2007). The effects of need for cognition on Internet use. *Computers in Human Behavior, 23*(1), 880–891.

Anacleto, R., Figueiredo, L., Almeida, A., & Novais, P. (2014). Mobile application to provide personalized sightseeing tours. *Journal of Network and Computer Applications, 41*, 56–64.

Awad, N. F., & Krishnan, M. (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.

Bandura, A. (1986). Fearful expectations and avoidant actions as coeffects of perceived self-inefficacy. *American Psychologist, 41*, 1389–1391.

Bansal, G., Zahedi, F., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138–150.

Barwise, P., & Strong, C. (2002). Permission-based mobile advertising. *Journal of Interactive Marketing, 16*(1), 14–24.

Belk, R. W. (2013). Extended self in a digital world. *Journal of Consumer Research, 40*(3), 477–500.

Brender, N., & Markov, L. (2013). Risk perception and risk management in cloud computing: results from a case study of Swiss companies. *International Journal of Information Management, 33*(5), 726–733.

Byron, K., & Laurence, G. A. (2015). Diplomas, photos, and tchotchkes as symbolic self-representations: understanding employees individual use of symbols. *Academy of Management Journal, 58*(1), 298–323.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: an empirical examination of the online consumer's dilemma. *Information Technology and Management, 6*(2–3), 181–202.

Chin, W. W., & Newsted, P. R. (1999). Structural equation modeling analysis with small samples using partial least squares. *Statistical Strategies for Small Sample Research, 2*, 307–342.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. *Organization Science, 10*(1), 104–115.

Danaher, P. J., Smith, M. S., Ranasinghe, K., & Danaher, T. S. (2015). Where, when, and how long: factors that influence the redemption of mobile phone coupons. *Journal of Marketing Research (JMR), 52*(5), 710–725.

Davenport, T. H., Mule, L. D., & Lucker, J. (2011). Know what your customers want before they do. *Harvard Business Review, 89*(12), 84–92.

Derlega, V. J., & Chaikin, A. L. (1977). Privacy and self-disclosure in social relationships. *Journal of Social Issues, 33*(3), 102–115.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents–measurement validity and a regression model. *Behaviour and Information Technology, 23*(6), 413–422.

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

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance—an empirical investigation. *The Journal of Strategic Information Systems, 17*(3), 214–233. http://dx.doi.org/10.1016/j.jsis.2007.09.002

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

Goodwin, C. (1991). Privacy: recognition of a consumer right. *Journal of Public Policy & Marketing, 10*(1), 149–166.

Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: consumers awareness and concerns. *Journal of Consumer Marketing, 19*(4), 302–318.

Gronli, T., Ghinea, G., & Bygstad, B. (2013). Exploring solutions for mobile companionship: a design research approach to context-aware management. *International Journal of Information Management, 33*(1), 227–234.

Han, S., Min, J., & Lee, H. (2015). Antecedents of social presence and gratification of social connection needs in SNS: a study of twitter users and their mobile and non-mobile usage. *International Journal of Information Management, 35*(4), 459–471.

Handler, S. M., Boyce, R. D., Ligons, F. M., Perera, S., Nace, D. A., & Hochheiser, H. (2013). Use and perceived benefits of mobile devices by physicians in preventing adverse drug events in the nursing home. *Journal of the American Medical Directors Association, 14*(12), 906–910.

Harman, H. H. (1976). *Modern factor analysis*. University of Chicago Press: Princeton, New Jersey.

Hong, I. B. (2015). Understanding the consumer's online merchant selection process. The roles of product involvement, perceived risk, and trust expectation. *International Journal of Information Management, 35*(3), 322–336.

Hsiao, C., Chang, J., & Tang, K. (2016). Exploring the influential factors in continuance usage of mobile social apps: satisfaction, habit, and customer value perspectives. *Telematics and Informatics, 33*(2), 342–355.

James, T. L., Warkentin, M., & Collignon, S. E. (2015). A dual privacy decision model for online social networks. *Information & Management, 52*(8), 893–908.

Jones, B. H., & Chin, A. G. (2015). On the efficacy of smartphone security: a critical analysis of modifications in business students practices over time. *International Journal of Information Management, 35*(5), 561–571.
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. http://dx.doi.org/10.1016/j.ijhcs.2013.08.016
Khasawneh, M. (2015). A mobile banking adoption model in the Jordanian market: an integration of TAM with perceived risks and perceived benefits. *Journal of Internet Banking & Commerce, 20*(3), 1–13.
Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544–564.
Kim, H. (2016). What drives you to check in on Facebook? Motivations, privacy concerns, and mobile phone involvement for location-based information sharing. *Computers in Human Behavior, 54*, 397–406.
Kock, N., & Lynn, G. S. (2012). Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. *Journal of the Association for Information Systems, 13*(7), 546–580.
Krasnova, H., Veltri, N. F., & Gunther, O. (2012). Self-disclosure and privacy calculus on social networking sites: the role of culture: intercultural dynamics of privacy calculus. *Business & Information Systems Engineering, 4*(3), 127–135.
LaRose, R., Rifon, N., Liu, S., & Lee, D. (2005). *Online safety strategies: a content analysis and theoretical assessment.*
Labrecque, L., Markos, E., & Milne, G. R. (2011). Online personal branding: processes, challenges, and implications. *Journal of Interactive Marketing, 25*(1), 37–50.
Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: a multidimensional developmental theory. *Journal of Social Issues, 33*(3), 22–42.
Lee, J. How brands build trust in a digital world. Huge. (2014, August 27). https://www.hugeinc.com/ideas/report/how-brands-build-trust-digitally Accessed 31.08.2015.
Lee, D., & LaRose, R. (2011). The impact of personalized social cues of immediacy on consumers information disclosure: a social cognitive approach, CyberPsychology. *Behavior & Social Networking, 14*(6), 337–343.
Lee, D. H., Im, S., & Taylor, C. R. (2008). Voluntary self-disclosure of information on the Internet: a multimethod study of the motivations and consequences of disclosing information on blogs. *Psychology & Marketing, 25*(7), 692–710.
Lee, E., Ahn, J., & Kim, Y. J. (2014). Personality traits and self-presentation at Facebook. *Personality and Individual Differences, 69*, 162–167. http://dx.doi.org/10.1016/j.paid.2014.05.020
Lee, N., & Kwon, O. (2015). A privacy-aware feature selection method for solving the personalization-privacy paradox in mobile wellness healthcare services. *Expert Systems with Applications, 42*(5), 2764–2771.
Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177–187.
Lee-Won, R. J., Shim, M., Joo, Y. K., & Park, S. G. (2014). Who puts the best face forward on Facebook?: Positive self-presentation in online social networking and the role of self-consciousness, actual-to-total Friends ratio, and culture. *Computers in Human Behavior, 39*, 413–423. http://dx.doi.org/10.1016/j.chb.2014.08.007
Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems, 51*(1), 62–71.
Li, Y. (2012). Theories in online information privacy research: a critical review and an integrated framework. *Decision Support Systems, 54*(1), 471–481. http://dx.doi.org/10.1016/j.dss.2012.06.010
Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems, 57*(1), 343–354.
Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management. *MIS Quarterly, 31*(1), 59–87.
Lin, T. C., Huang, S. L., & Hsu, C. J. (2015). A dual-factor model of loyalty to IT product—the case of smartphones. *International Journal of Information Management, 35*(2), 215–228. http://dx.doi.org/10.1016/j.ijinfomgt.2015.01.001
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.
Martins, C., Oliveira, T., & Popovic, Al. (2014). Understanding the Internet banking adoption: a unified theory of acceptance and use of technology and perceived risk application. *International Journal of Information Management, 34*(1), 1–13.
Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing, 18*(3), 15–29.
Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing, 19*(2), 206–215.
Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers protection of online privacy and identity. *Journal of Consumer Affairs, 38*(2), 217–232.
Misoch, S. (2015). Stranger on the internet: online self-disclosure and the role of visual anonymity. *Computers in Human Behavior, 48*, 535–541.
Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: evidence from Malaysia. *Computers in Human Behavior, 28*(6), 2366–2375. http://dx.doi.org/10.1016/j.chb.2012.07.008
Morosan, C. (2015). Understanding the benefit of purchasing ancillary air travel services via mobile phones. *Journal of Travel & Tourism Marketing, 32*(3), 227.
Morosan, C., & DeFranco, A. (2015). Disclosing personal information via hotel apps: a privacy calculus perspective. *International Journal of Hospitality Management, 47*, 120–130.
Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100–126.
Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903.
Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: problems and prospects. *Journal of Management, 12*(4), 531–544.
Rönkkö, M., & Ylitalo, J. (2011). PLS marker variable approach to diagnosing and controlling for method variance. In *Proceedings of International Conference on Information Systems.*
Rui, J., & Stefanone, M. A. (2013). Strategic self-presentation online: a cross-cultural study. *Computers in Human Behavior, 29*(1), 110–118. http://dx.doi.org/10.1016/j.chb.2012.07.022
Stone, E. F., & Stone, D. L. (1990). Privacy in organizations: theoretical issues, research findings, and protection mechanisms. *Research in Personnel and Human Resources Management, 8*(3), 349–411.
Sun, Y., Wang, N., Shen, X., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior, 52*, 278–292.
Sutanto, J., Palme, E., Tan, C. H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users. *MIS Quarterly, 37*(4), 1141–1164.
Taylor, D., Davis, D., & Jillapalli, R. (2009). Privacy concern and online personalization: the moderating effects of information control and compensation. *Electronic Commerce Research, 9*(3), 203–223. http://dx.doi.org/10.1007/s10660-009-9036-2
Vanden, A. M., Antheunis, M. L., & Schouten, A. P. (2014). Me, myself and my mobile: a segmentation of youths based on their attitudes towards the mobile phone as a status instrument. *Telematics and Infomatics, 31*(2), 194–208.
Wang, Y., Wu, S., Lin, H., & Wang, Y. (2011). The relationship of service failure severity, service recovery justice and perceived switching costs with customer loyalty in the context of e-tailing. *International Journal of Information Management, 31*(4), 350–359.
Xu, D. J., Liao, S. S., & Li, Q. (2008). Combining empirical experimentation and modeling techniques: a design research approach for personalized mobile advertising applications. *Decision Support Systems, 44*(3), 710–724. http://dx.doi.org/10.1016/j.dss.2007.10.002
Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing. *Decision Support Systems, 51*(1), 42–52. http://dx.doi.org/10.1016/j.dss.2010.11.017
Xu, H., Teo, H. 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.
Ringle, C.M., Wende, S., Will, A. 2005. SmartPLS 2.0 (beta) Hamburg.
Millward, S. (2014). China now has 520 M smartphone users, will top 700 M by 2018. https://www.techinasia.com/china-520-million-smartphone-users-2014/ Accessed 26.05.2015.
Fingas, J. Two-thirds of Americans now have smartphones. 2014 http://www.cnet.com/news/worldwide-smartphone-user-base-hits-1-billion/ Accessed 26.5.2015.
International telecommunication union the world in 2013: ICT facts and figures (2013). http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf Accessed 12.05.2015.
Boyles, J.L., Smith, A., Madden, M., Privacy and data management on mobile devices Pew Research Center 2012, Sept. 5 Available from: http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/ Accessed 19.02.2016.
Dinev, T., Hart, P. (2003, August) Privacy concerns and internet use—A model of trade-off factors. In Academy of Management Proceedings (vol. 2003, No. 1, pp. D1–D6). Academy of Management.

Further reading

Fan W., & Gorden M.D. (2014). The power of social media analytics. *Communications of the ACM, 57*(6), 74–81.

Tien Wang is an assistant professor at the Institute of International Management at National Cheng Kung University in Taiwan. She received her Ph.D. in Business Administration at the University of Texas at Arlington. Her research interests include digital consumer behavior, social commerce, and marketing finance interface. Her works have been published in International Journal of Human-Computer Interaction, Journal of Information Management, Taiwan Journal of Marketing Science, and various conference proceedings.

Trong Danh Duong is a graduate of the Institute of International Management at National Cheng Kung University in Taiwan.

Charlie C. Chen received his Ph.D. in Management Information Systems from Claremont Graduate University. Dr. Chen is a professor in the Department of Computer Information Systems and Supply Chain Management at Appalachian State University. His current research interests are project management and supply chain management. He is a Project Management Professional certified by the Project Management Institute. Dr. Chen has authored more than 100 referred articles and published in such journals as International Journal of Project Management, IEEE Transactions on Engineering Management, Behaviour and Information Technology, Communications of Association for Information Systems, and Journal of Global Information Technology Management.