林東清[*] 徐士傑[**] 陳耕硯[***] 吳盛[****]

探討下載適地性服務手機應用程式影響因素之研究

（本篇為英文論文，全文請參閱第 **49-68** 頁）

研究目的：本研究目的想要探討使用者一方面基於使用適地性服務 App 的好處，另一方面又害怕對於個人位置資訊不當使用的風險。因此我們使用隱私計算理論來探究其使用者行為模式，並進一步深入了解付費與免費對於使用者的隱私計算有何影響。

研究設計/方法：總共收集 425 份線上問卷，刪除無效問卷後共有 418 份有效問卷，並使用 Smart PLS 2.0 統計軟體檢測其研究假說成立與否。

研究結果：與娛樂型 App 相比，使用者會比較注重工具型 App 所能帶來的好處。和工具型 App 相比，使用者會比較擔心娛樂型 App 的潛在風險；然而付費 App 會讓使用者十分重視 App 所能帶來的好處，況且比起工具型 App 會更為重視娛樂型 app 的風險。假若是免費的 App，使用者會比較重視工具型 App 的好處。

研究限制/啟發：本研究主要是針對 Android 平台的用戶，所以 IOS 平台用戶的行為可能會有所不同。

理論/實務/社會意涵：娛樂型的手機應用程式提供商必須保證其安全性或者要說明手機應用程式如何存取要求使用的權限，不然使用者會因隱私洩露的風險降低下載的意願。

創見/價值：由於過去的研究很少討論付費型與免費型的手機應用程式對使用者隱私風險的影響，因此本研究提供這兩種不同情境做深入的探討。

關鍵字：隱私計算、適地性服務、手機應用程式、科技接受模式、口碑推薦

[*] 林東清為國立中山大學資訊管理學系專任特聘教授
[**] 徐士傑為國立中山大學資訊管理學系專任教授
[***] 陳耕硯為國立中山大學資訊管理碩士，目前任職於財團法人資訊工業策進會
[****] 吳盛為南臺科技大學資訊管理系專任副教授(通訊作者) Email: shengwu@stust.edu.tw

Tung-Ching Lin* Jack Shih-Chieh Hsu** Ken-Yen Chen*** Sheng Wu****

A Study on the Factors Affecting Downloading of Location Based Services Mobile Applications

(Received Oct 27, 2020; First Revision Nov 28, 2020; Accepted May 25, 2021)

Abstract

Purpose – The purpose of this paper is to find out if users may be attracted by the benefits of location based services (LBS) app's functions, otherwise, users may have stopped by the perceived risks of the LBS app. Thus, we use privacy calculus theory to explain user behaviors in this context. Furthermore, we were to determine the impact of paid or free and app category on privacy calculus.

Design/methodology/approach – A total of 425 people responded to our online questionnaire. After dropping invalid or incomplete responses, only 418 surveys were considered valid. We adopted Smart PLS 2.0 to calculate the β coefficients and significance levels of all the proposed hypotheses.

Findings – First, whether paid or free makes a difference to the user's privacy calculus depends on the app category. In the paid condition, users focus on the privacy disclosure benefits. This means that users will critically consider the app's functionality. Users also attach importance to the privacy disclosure risks of hedonic apps. In the free condition, users attach more importance to the privacy disclosure benefits of utilitarian apps. Second, the app category also impacts the user's privacy calculus. Users focus on the benefits of a utilitarian app and they pay more attention to the risks of a hedonic app.

Research limitations/implications – Our research focused on users of the Android platform, but the behaviors of IOS platform users might be different.

Practical implications/Social implications – Vendors of hedonic apps must either guarantee the security of their app or explain how the requested permissions are used by the app. Otherwise, the privacy disclosure risks decrease users' intention to download the app.

Originality/value – Since there is almost no research discussing the effects of paid or free and app category on privacy risks, our research is the first to provide insight regarding these two constructs in this context.

Keywords – privacy calculus, location based services, app, technology acceptance model, word of mouth

For full paper, please go to
https://www2.management-review.org/all-issues

---

* Tung-Chin Lin is currently a Distinguished Professor in the Department of Information Management at National Sun Yat-sen University, Taiwan.

** Jack Shih-Chieh Hsu is currently a Professor in the Department of Information Management at National Sun Yat-sen University, Taiwan.

*** Ken-Yen Chen is currently employed by the Institute for Information Industry. He received his Master's degree in Information Management from National Sun Yat-sen University.

**** Sheng Wu is currently an Associate Professor in the Department of Information Management at Southern Taiwan University of Science and Technology, Taiwan. (Corresponding Author) Email: shengwu@stust.edu.tw

DOI:10.6656/MR.202107_40(3).ENG049

1. Introduction

The internet and mobile technology have become part of everyday life. Smartphones, in particular, are ubiquitous in many countries. The popularity of the smartphone has facilitated greater diversity in location based services (LBS). LBS means service providers base their software's functionality on the user's geographic information and preferences to provide a real-time location data. Such as services include emergency and security related services, entertainment, navigation, property tracing, city guides, traffic reports, and location-based advertising. By extension, LBS can be defined as the integration of mobile devices and location-based information in order to provide added value to internet services. The advancement of wireless internet and mobile phones has made LBS a worldwide phenomenon (Rao and Minakakis 2003). Thus, the popularity of smartphones makes LBS an industry which demands further attention.

Nevertheless, the growth of the LBS market and its related services is accompanied by increasing concerns over privacy, since personal location information can be used inappropriately (Chen et al. 2017; Junglas and Watson 2008; Wang and Lin 2017; Wang, Sun, and Huang 2018). For example, Android and iPhone apps usually ask users to allow such information to be collected in order to improve the app. Some malicious providers use their apps to collect users' information, threatening users' privacy. Users desire to use an LBS app because it is useful and offers economic benefits. After weighing the risks, users may choose to allow access to their personal information in exchange for the benefits of the LBS app, but only if the benefits outweigh the risks.

Many studies have noted that privacy concerns and privacy risks negatively impact the intention to use LBS, though these studies were based on the early mobile LBSs, which had limited functionality. At that time, smartphones were not widely available (Keith et al., 2010; Xu and Gupta 2009; Zhou 2012). In recent years, the rapid development of the mobile platform has given malevolent app developers increased opportunities for financial gain, so security breaches have happened with greater frequency. Malevolent apps often send fake social network service messages or trace the user's private data in order to invade the user's privacy, or gain illicit access to the user's financial accounts. Enhancing privacy policies and adding user-friendly technology features, such as "do-not-track" and the controllable GPS, would decrease privacy problems. However, privacy is still a major concern, because once the user's location information has been collected by an app company, users find it difficult if not impossible to control that information. For instance, Apple was investigated for secretly recording iPhone and iPad users' locations in hidden files on their devices, which was cause for significant security and privacy concerns (O'Reilly 2011). As long as LBS is associated with a concern for privacy, significant resistance will have to be overcome before LBS is universally accepted.

In order to provide localization service, LBS apps have to know the user's position, so they must request "location" permission, at least. However, some malicious apps exist in the app store. Some apps are designed to check the smartphone's state and identity, so they can run without being interrupted by an incoming phone call. Unfortunately, these permissions can be used by Trojan apps to execute malicious behaviors, like recording the user's phone conversations and sending the device's International Mobile Equipment Identity information to an assigned server.

LBS is a popular new service whose functions and convenience are beyond all doubt, but because it requests position information, which raises user's misgivings regarding privacy, it then becomes a privacy risk. Thus, the market penetration rate of LBS apps is still low. To determine how this penetration rate could be increased, we explore the factors that might increase users' LBS app download intentions. Recent studies have noted that if the benefits users gain from a transaction are relevant to the personal information being disclosed, users are willing to use the service. For this reason, the permissions requested by online vendors must be relevant to the content of their service (Xu et al. 2009). We suggest that both perceived usefulness and perceived ease of use are the key benefits for which users will disclose private information. On the other hand, if the permissions requested by an LBS app include sensitive information or are irrelevant to the app's functionality, this might lead to a privacy risk. As mentioned above, users can judge the app's benefits and risks via the ratings and comments, so we believe that word of mouth (WOM) will influence both the benefits and risks of disclosing private information.

Besides perceived usefulness and perceived ease of use, cost is a very important consideration before using any technology. Downloading apps is no different. When downloading an app, users have to consider its costs. The higher the cost, the greater the risk perceived by the users, thus decreasing the intention to download. Users also evaluate the benefits and risks of downloading paid apps, in order to avoid unnecessary monetary losses. Therefore, we believe that when considering downloading paid apps, users are more aware of the benefits and risks of disclosing private information. On the other hand, free apps have essentially no monetary cost, so users might focus more on the privacy risks of such apps.

The purpose of this research is to find out if users are more aware of the benefits or the risks of disclosing private information in each of these conditions. On one hand, users may be attracted by an LBS app's functions and benefits, while on another hand, users may be afraid of the perceived risks of the LBS app. Many studies have applied privacy

calculus theory for analyzing users' privacy concerns (Culnan 1993; Dinev and Hart 2006; Hann et al. 2007; Hui, Teo, and Lee 2007; Kim, Yoon, and Zemke 2017; Milne and Gordon 1993). According to these studies, users first consider all factors related to a given information disclosure situation in order to analyze the benefits and risks, and then evaluate their privacy concerns. Thus, we use privacy calculus theory is appropriate to explain user behaviors in this context. Furthermore, whether the app is paid or free is an important issue for the vendor about to publish a new app. Many past studies have discussed the differences between hedonic and utilitarian products, and have proved that these different product types influence a user's use intention (Beckmann 2016; Kim et al. 2014; Xiang et al. 2015). Thus, we examine how the factors of cost (paid vs. free) and app category (hedonic vs. utilitarian) impact users' privacy calculus under different conditions.

2. Literature Review and Hypotheses Development

2.1 Privacy Calculus

Privacy calculus is inferred from classic theories on information technology (IT) adoption, such as the theory of reasoned action (TRA) (Ajzen and Fishbein 1980), the technology acceptance model (TAM) (Davis 1989), and the theory of planned behavior (TPB) (Ajzen 1991). In particular, their concepts are all based on the factors of cognition and trust of technology, and how they impact behavioral intention. The concept of privacy calculus involves trust which increases users' intention to disclose personal information in order to perform transactions on the internet (Wottrich, Reijmersdal, and Smit 2018). Previous studies focused on factors which would motivate users to willingly disclose location information in order to receive the benefits of LBS (Kim Yoon, and Zemke 2017).

However, in contrast to the TRA, the TPB and the TAM, privacy calculus suggests that usage intention is affected by beliefs which are actually in opposition to each other. In the other words, when deciding whether or not to use LBS, users consider not only the service's usefulness and ease of use, but also the relative risk of disclosing their location. Hence, when users make this decision, they first calculate the risk involved in obtaining the benefits (Keith et al. 2010; Palos-Sanchez, Hernandez-Mogollon, and Campon-Cerro 2017).

Many studies have applied privacy calculus structure to marketing and social networks. This is because the viewpoint of privacy calculus has been used in studies discussing users' privacy concerns (Culnan and Bies 2003). This privacy calculus perspective has been found to be the most useful structure for analyzing users' privacy concerns (Culnan 1993; Dinev and Hart 2006; Hann et al. 2007; Hui, Teo, and Lee 2007; Kim, Yoon, and Zemke 2017; Milne and Gordon 1993). According to these studies, users first consider all factors related to a given information disclosure situation in order to analyze the benefits and risks, and then evaluate their privacy concerns.

Individuals must usually make privacy decisions when personal information is required in exchange for some benefit or reward (Laufer and Wolfe 1977; Stone and Stone 1990). In other words, when the disclosure of personal information is traded for some benefit, the perspective of information privacy calculus can be used to explore users' evaluations of the benefits and risks of this disclosure. We argue that as long as users feel that they will be given positive feedback (e.g., the benefits are greater than the losses caused by disclosure), they are likely to accept the risks of disclosing personal information (Culnan and Bies 2003; Kim et al. 2019; Trepte, Scharkow, and Dienlin 2020).

2.2 Privacy Disclosure Risk

In case of e-commerce, when users face uncertainty, or have uncomfortable or anxious feelings, their perception of the risk is thought to have a negative impact on their evaluation and adoption of products or services (Dowling and Staelin 1994). There are many aspects to the construct of perceived risk (e.g., effect, financial, time, security, social and psychological losses), and all of them are related to the results of the risk (Cunningham 1967). Featherman and Pavlou (2003) focused on electric devices and added the concept of privacy risk, which is an important aspect of risk and is defined as an individual's belief in the degree of potential loss caused by disclosing his or her personal information (Malhotra, Kim, and Agarwal 2004). Therefore, we employ perceived privacy disclosure risk as a one-dimensional construct and define it as the perception of potential loss caused by giving personal information to an LBS service vendor.

Previous privacy literature definitions came from the perspective of organizations, including granting unauthorized access and selling personal data to or sharing information with a third party, financial institution or government agency (Otjacques, Hitzelberger, and Feltz 2007). Many privacy studies have confirmed that perceived privacy risks negatively influence the intention to disclose personal information in a network transaction (Xu et al. 2009). LBS articles have noted that inappropriate handling of personal information might allow location information to be matched with someone's personal identity (Clarke 2001). Thus, if users feel that their personal information is not protected effectively or that there is a high risk of a privacy violation, they may not want to disclose personal information to the LBS.

LBS can use location information to provide various personalized services which can reflect individual taste and preferences. However, the more personalized the service becomes, the greater the chances of increasing the privacy violation risk (Oh, Jung, and Park 2014). Our study explores the possibility that perceived privacy disclosure risk is the major factor impacting a user's willingness to provide personal information to an LBS vendor, and that the concern for privacy is one of the important factors affecting privacy disclosure risk.

Previous research has shown that perceived risk includes privacy risk (Malhotra, Kim, and Agarwal 2004). Perceived privacy risk refers to the user's sense that a potential loss can be incurred if personal information is disclosed (Featherman and Pavlou 2003). Perceived privacy risk is a one-dimensional construct which is used to measure the loss of control of specific personal information (Xu et al. 2009). We use the construct of privacy disclosure risks to measure the risk involved in the disclosure of location data or other private information.

Studies have confirmed that perceived privacy risk negatively influences users' behavioral intention to disclose personal information in an electronic commerce context (Dinev and Hart 2006; Malhotra, Kim, and Agarwal 2004). When online users perceive that a certain behavior is more risky, their intention to use the online product, service or website decreases, thus decreasing the usage rate (Liao et al. 1999). If consumers perceive online shopping as risky, their online shopping intention is negatively influenced (Forsythe and Shi 2003; Lee and Tan 2003).

Krasnova, Hildebrand, and Guenther (2009) noted that perceived privacy risk is a major factor for predicting the likelihood of a user disclosing personal information in a social network. We apply their result to our research, and suggest that users consider the perceived privacy risk, this decreases their intention to download the app. Privacy disclosure risk is thus defined as a user's perception of the expected negative consequences of disclosing personal information in an LBS app. Therefore, this paper posits hypothesis one.

H1: Privacy disclosure risks negatively affect download intention.

2.3 Privacy Disclosure Benefits

The expected benefits are believed to have a positive influence on users' willingness to disclose personal information to an LBS. Location based services belong to the category of context-aware computing applications, so they employ the user's location, identity, activity and a timestamp to send user-specific information to the service in order to provide a contextualized value (Bellavista, Küpper, and Helal 2008).

The locatability construct reflects the LBS's time-variation value and location-variation value. Locatability is defined as the perceived value of the user's ability to access the required information and service at the right time and in the right place. Hence, locatability can turn an app's use of location and time into a major advantage to entice users to disclose their personal information so these users can access the information or service they need anytime and everywhere (Barnes 2003; Junglas and Watson 2006; Junglas and Watson 2008).

Another attractive benefit of LBS is personalization value, which emphasizes individualized functions to enhance the user experience and increase the fluidity of interacting with the app (Zimmermann, Specht, and Lorenz 2005). In the literature, the term LBS personalization means that the LBS can be suited to individual user's activity content, interests and needs. Users might thus be encouraged to disclose their personal information in exchange for personalized service and information (Xu et al. 2009).

According to Chellappa and Sin (2005), people use personalized online services when they can balance their privacy concerns with the perceived value of the personalized service. The conclusion is that users might give up a certain degree of privacy in order to obtain the potential benefits of locatability and personalization.

As mentioned before, the benefits of LBS are that it can use locatability features to provide a personalized experience and personalized information. Research has shown that perceived benefits positively influence a user's privacy disclosure intention in the context of LBS (Bellavista, Küpper, and Helal 2008). Culnan and Bies (2003) noted that if users believe they will receive positive feedback, they are likely to sacrifice by incurring some privacy risk. Besides, users might be enticed by the benefits to be gained by disclosing their private information, and thus use their personal information in exchange for such benefits (Xu and Gupta 2009). We suggest that the benefits of an LBS app induces users to download the LBS app. Therefore, this paper posits hypothesis two.

H2: Privacy disclosure benefits positively affects download intention.

2.4 Information Sensitivity

Our study proposes that making privacy decisions involves more than the above-mentioned risk/benefit analysis. Information disclosure involves a significant amount of uncertainty, and this condition allows users to be easily cheated by internet vendors or websites. The perceived risk can cause users to worry that private, sensitive

information might be revealed to malicious people. Since LBSs encounter this same condition, we suggest that the factor of sensitive information affects a user's perception of the privacy disclosure risk. We define sensitive information as "the degree to which the user feels anxiety regarding the disclosure of specific personal information to others" (in our case, to an LBS app) (Metzger 2004). Users feel considerably more risky when disclosing sensitive information than when disclosing less sensitive information (Jalilvand et al. 2012)

We consider giving an app permission to access information such as "location" to be a kind of information disclosure. According to social network disclosure studies, the major cost of disclosure in that context is the concern that private, sensitive information may be obtained by cruel people (McKnight, Lankton, and Tripp 2011). When a service vendor is allowed to access a lot of potentially sensitive information, privacy concerns become particularly prominent. Hence, when using an LBS, users might continuously judge and weigh the risks and benefits of privacy disclosure.

Information sensitivity refers to the degree to which the disclosure of a user's personal data to unreliable or malicious persons can result in terrible consequences. Previous research has shown that if users consider the information to be sensitive, they decrease their intention to disclose such information (Yang and Wang 2009). Jalilvand et al. (2012) found that people feel that they are being more risky when they disclose sensitive information as opposed to general information. Malhotra, Kim, and Agarwal (2004) proved that the more sensitive the information requested, the more negative the effect on the user's attitude and intention to disclose personal information.

Many types of permission can be requested by apps in Google Play, some of which are sensitive (e.g., location, contacts) and some of which are not sensitive (e.g., in-app purchases, Wi-Fi connection information). Thus, we expect users to be unwilling to provide sensitive information, because of the negative consequences of such information being abused. Hence, we propose that when the permissions requested by the LBS app involve sensitive information, users might feel that downloading the app is risky, and thus decrease their download intention. Therefore, this paper posits hypothesis three.

H3: Information sensitivity positively influences privacy disclosure risks.

2.5 Permission Irrelevance

LBS vendors should fulfill fair information practices rules to enhance perceived fairness and reduce the privacy loss incurred by users' disclosure of information. Network users generally care about the amount and depth of their information that is collected by network vendors. This means that the collected information should be relevant to the benefits for which it is being exchanged (Li, Sarathy, and Xu 2010). Since LBS belongs to the same category as network services, LBS users might care about the amount and depth of their information that is collected by an LBS vendor. As such, the information collected by an LBS should also be relevant to the benefits for which it is exchanged. In this research, we define this as the level of requested permissions fit the LBS app functions.

Apps must request some permissions to run certain functions that require user data. However, Zhou (2012) found that users are afraid that the collected information might be abused. The permissions which involve privacy raise users' privacy concerns (Dinev and Hart 2006). Therefore, the permissions requested must be relevant to the app's functionality for the users to consider the request to be fair. The determination of the exchange's fairness and the risk/benefit analysis are separate but related factors affecting users' willingness to disclose personal information. As discussed before, besides the risk/benefit analysis, another topic of online information disclosure is the perceived fairness involved in the disclosure of information. The fairness of the information exchange is defined as the collected information relating to the functions of the system. In other words, if the permissions requested by the system are not related to the system's functions, users consider the disclosure of information to be risky. Therefore, this paper posits hypothesis four.

H4: Permission irrelevance positively influence privacy disclosure risks.

2.6 Word-of-Mouth (WOM)

WOM is an activity in which users analyze, remember and explain things, then communicate and share meaningful information with others (Weiner 1985). WOM is a result of an emotional response to a consumer situation (Swan and Oliver 1989). It might be positive, neutral or negative (Anderson 1998). WOM is a reliable and powerful information source in marketing. For example, In Google Play, users can view other users' comments, their ratings of the app, and the number of times the app has been downloaded. This information reveals a specific viewpoint about users' perceptions of the app. Although social comments and ratings mainly reflect the app's perceived usefulness and efficacy, they seldom discuss risk, but users still have to rely on others' comments and ratings to identify malicious apps and any potential risks. We consider such comments and ratings as a kind of WOM.

If developers have a thorough understanding of this discussion, they will avoid the problem of low ratings, and guarantee their quality. User feedback has become an important means by which to understand users' perceptions of the app. Actually, Parasuraman, Zeithaml, and Berry (1994) proved that when consumers shop on Amazon.com, an online retailer, the comments and messages of others play an important role in the consumers' purchase decision. Harlam et al. (1995) found that user feedback is a key determinant of the intention to purchase an app. Mazumdar and Jun (1992) mined 30,000 BlackBerry apps, and found that an app's rating is strongly related to the number of times the app has been downloaded. Chong et al. (2018) found that user relied heavily on ratings to guide their app selections. Thus, users tend to rely on the opinions and ratings of other users to reduce uncertainty of risk (Kim, Kankanhalli, and Lee 2016).

Since online transactions involve a high level of uncertainty, users need reliable and useful information about the product to support their purchase decision (Simonin and Ruth 1995). In emerging markets, user feedback plays an important role in purchase decisions (Krasnova, Hildebrand, and Guenther 2009). Since online feedback affects online shopping behaviors (Yang and Wang 2009; Yoo, Sanders, and Moon 2013). Previous studies have pointed out that WOM has an important effect on users' decisions (Arndt 1967; Richins and Root-Shaffer 1988). Other studies have shown that, in a travel context, WOM positively influences a user's attitude to the service or products (Albarq 2014; Jalilvand et al. 2012). Thus, we can deduce that WOM will influence a user's privacy calculus.

In this study, the comments, ratings, and number of downloads represent other users' evaluations of the app. According to the literature review, these factors are a kind of WOM. Therefore, we suggest that if the ratings of the app are high, users consider the app to be helpful and low risk. However, if ratings are low, users might consider the app not to be useful and expect it to involve some risk. Comments are used similarly: if most of the comments regarding the app are positive, users consider the app to be good. The inverse is also true. The number of downloads is an indicator of the popularity of the app, which we suggest, has the same effect. Based on the discussion, above, this paper posits hypotheses five.

H5a: WOM negatively influences privacy disclosure risks.

H5b: WOM positively influences privacy disclosure benefits.

2.7 Technology Acceptance Model (TAM): Perceived Usefulness and Perceived Ease of Use

The TAM may be the most often used theory in studies of user acceptance of mobile commerce. It has been used to study mobile shopping (Albarq 2014), mobile ticketing (Mallat et al. 2008), digital multimedia broadcasting (Jung, Perez-Mira, and Wiley-Patton 2009; Kim, Shin, and Lee 2009), 3G services (Luarn and Lin 2005), and mobile games (Radner and Rothschild 1975). Perceived usefulness is an external motivation for accepting a new information technology (Davis, Bagozzi, and Warshaw 1992; Venkatesh 2000), and is an important determining factor in users' acceptance of mobile service (Hong and Tam 2006; Kim, Chan, and Gupta 2007; Mallat et al. 2008; Nysveen, Pedersen, and Thorbjørnsen 2005; Pagani 2004).

Perceived usefulness and perceived ease of use are very critical determining factor in TAM. Previous studies have pointed out that perceived usefulness is an important predicting factor of technology adoption. Since its introduction, the TAM has been repeatedly applied and verified, and has generated a significant amount of feedback. One of the most influential research models in IT adoption research is TAM model (Chau 1996). The TAM's construct of perceived usefulness originally referred to work-related productivity, performance and effectiveness (Davis 1989). This is an important conviction, which means it can provide a diagnostic viewpoint for how a user's attitude influences both usage and use intention. Perceived usefulness indirectly affects use intention through attitude (Davis 1989; Davis 1993; Taylor and Todd 1995). It includes the concepts of expectancy theory. Triandis (1980) mentioned that expected result is an important factor affecting behavior. Individuals use perceived usefulness to evaluate the result of their behaviors, and then make the decision.

In accordance with Davis (1989), we define perceived usefulness as users' belief that the downloaded app will be helpful. Venkatesh and Davis (2000) found that perceived usefulness has a significant effect on initial usage. Many studies have validated that perceived usefulness effects the intention to adopt m-commerce (e.g., Luarn and Lin 2005). Gefen, Karahanna, and Straub (2003) found that perceived usefulness influences users' online purchase intention and their willingness to disclose personal information. Moreover, perceived usefulness increases online users' willingness to give up some privacy in order to get the benefits from products or services (Li, Sarathy, and Xu 2010). Therefore, this paper posits hypothesis six.

H6: Perceived usefulness positively influences privacy disclosure benefits.

Studies have shown that perceived ease of use significantly affects willingness to adopt new technology (Davis 1989). Perceived ease of use refers to the fact that users think the technology is easy to use so they don't need to learn much (Davis 1989). Effort is a limited resource, and people will allocate it to the activities that they can afford (Radner and Rothschild 1975). All else being equal, users will adopt the technology that is easiest to use. When a technology is hard to use, it imposes an important barrier to user adoption (Venkatesh 1999; Venkatesh 2000). Perceived ease of use is one factor users consider when they are about to download an app, because they hope the app will also be easy to use. Smartphones have some specific constraints, such as a small screen, so unless the app presents an easy-to-use interface, people will not want to use it (Lee and Benbasat 2004; Zhang, Rau, and Salvendy 2010). If the app is easy to use, users can skillfully use the app, which can reduce the cost of learning the app, and allow users to quickly get the benefits of the app. Thus, we suggest that perceived ease of use will have a positive influence on privacy disclosure benefits. Therefore, this paper posits hypothesis seven.

H7: Perceived ease of use will have a positively influences on privacy disclosure benefits.

2.8 Paid or Free

In the context of traditional service industry marketing, researchers have found that another factor besides service quality affects customer satisfaction: the sacrifice the user makes in order to gain the benefits. Most previous studies have focused on satisfaction or customer loyalty. Recent technology adoption related studies have suggested that the cost factor should be taken into consideration. In economic terms, shoppers generally see price as a critical financial cost factor (Zeithaml 1988). According to the research, when users want to download an app, they consider whether or not it is free. Most users tend to use free apps. This study proposes that charging a fee for an app decreases users' intention to download the app. Hair et al. (1998) found that product price limits the selectivity of a purchase, and could increase the financial risk. However, many studies have found that price also has a positive effect. For example, customers use price to judge the quality of product. Hence, the higher the price, the greater the purchase intention. Sweeney and Soutar (2001) proved that the higher the perceived price, the greater the perceived quality of the product, which increases consumers' purchase intentions. Previous studies have noted that if the product is not well known, consumers decrease their potential risk by using price as an indicator by which to judge the product's service level and quality (Ji 2013; Metzger 2004).

When downloading apps in Google Play, users can view whether the apps are paid or free, and they can judge each app only by its related information. As mentioned before, price is an important evaluation factor when users are not familiar with the product or service (Parasuraman, Berry, and Zeithaml 1991; Parasuraman, Zeithaml, and Berry 1994). One study indicated that people limit their purchase selections based on price, and price alone can increase the financial risk of purchasing, decreasing users' intention to purchase. Nevertheless, many studies have found that price also has positive effects (Kaplan Szybillo, and Jacoby 1974).

Therefore, we propose that whether an app is paid or free influences users' privacy calculus before they download the app. If the app is paid, users consider carefully whether or not to download it, which might influence privacy calculus. On the other hand, if the app is free, users might not consider carefully. Since most apps provide a free trial edition, and also have a paid version with full functionality, people generally consider the functionality of paid apps to be better, and expect paid apps to be safer than free apps. Therefore, this paper posits hypotheses eight.

H8a: The impact of privacy disclosure risks on download intention is greater when the app is free than when the app is paid.

H8b: The impact of privacy disclosure benefits on download intention is greater when the app is paid than when the app is free.

2.9 App Category

According to previous studies, product features influence consumers' purchase intentions regarding an entire series of products (Harlam et al. 1995; Mazumdar and Jun 1992; Simonin and Ruth 1995). Many customer behavior studies have indicated that certain specific product categories can evoke customers' emotional needs, so researchers have divided products into two classifications: hedonic and utilitarian (Beckmann 2016; Strahilevitz 1999). Hedonic products are those which are intended for entertainment-oriented consumption, and which consumers find interesting and seek for a sense of enjoyment (Xiang et al. 2015). Utilitarian products are those which are intended for target-oriented consumption, and which consumers use to fulfill some basic need or functional mission (Kim et al. 2014). Thus, utilitarian or hedonic products provide cognitive or emotional benefits to the consumer, respectively, both of which influence the purchase decision.

Apps can also be clearly separated into two categories: games and tools, which correspond directly to the hedonic and utilitarian categories, respectively. Though previous studies have not discussed this issue, we propose that a user's

privacy calculus differs depending on which of these two categories applies to the app being considered. We suggest that people generally place importance on the functionality of utilitarian apps, which means they pay closer attention to the privacy disclosure benefits. If the app is very useful or helpful, the user will still be willing to download it, despite the privacy risk. Users do not consider hedonic apps to be necessary, so we suggest that if a game appears to have a high level of privacy disclosure risk, users might forego that game and search for another. Therefore, this paper posits hypotheses nine.

H9a: The impact of privacy disclosure risks on download intention is greater for hedonic apps than for utilitarian apps.

H9b: The impact of privacy disclosure benefits on download intention is greater for utilitarian apps than for hedonic apps.

Finally, based on the above literature review, this study proposed a research model (Figure 1) to understand the interactions among the app download intention, privacy disclosure risks, privacy disclosure benefits, information sensitivity, permission irrelevance, WOM, perceived usefulness, perceived ease of use, paid or free, and app category.

3. Research Method

3.1 Sampling

The data of this research were shared via Facebook, and responders were requested to participate in our survey via Facebook messenger. To determine the effect of paid or free and app category on users' privacy calculus, we adopted the online questionnaire method. In order to encourage more people to complete the research questionnaire and increase the number of valid responses, we provided a lottery draw with 25 coupons to 7-Eleven, worth NT$100 each, as a reward. Since WOM is an objective construct, we were concerned that there would be no differences in the perceptions of the questionnaire recipients, which would make the answers too similar. Hence, we changed this to ratings, comments, and number of downloads. Ratings were divided into low ratings (1.5 stars), medium ratings (3.5 stars) and high ratings (4.5 stars). All comments were actual comments in Google Play, which we separated into positive comments and negative comments. Downloads, information sensitivity, permission irrelevance, perceived ease of use, and perceived usefulness are subjective, so we did not change those in our scenario. We used 2 (paid or free) *2 (app category) *3 (ratings) to develop 12 different scenarios. High ratings and positive comments were attributed to famous vendors (Google, SEGA). Low ratings and negative comments were attributed to the vendors whose names we created (GoTravel, LBS Play). One of the medium ratings was attributed to the famous vendors (Google, SEGA), and the other medium rating was attributed to our fictitious vendors (GoTravel, LBS Play). For the medium ratings scenario, and half of comments were positive and half were negative.

Additional, we found two LBS apps to represent the two app categories. The utilitarian one was a navigation app, and the hedonic app was a treasure game. We used the original apps' pictures and introductions, changing only the name of the vendor. The price of each paid app was set to NT$89. We also did not change the permissions requested by the apps. Since both apps requested access to the phone's camera and microphone, recipients could judge whether or not the permissions were relevant (see Figures 2 and 3).

Finally, the online survey was conducted over the two-week period. After respondents entered our website, they were directed to a randomly selected scenario. They saw the introduction to this questionnaire experiment, and were then allowed to enter the questionnaire scenarios. The scenarios show a short story to guide respondents into the scenario. The app install page from Google Play was then displayed. The next page showed the permissions requested by the app, with a short description above reminding respondents to pay attention to the permissions. Respondents were then allowed to press Next to proceed to the questionnaire. A total of 425 people responded to our questionnaire, but it is likely that some recipients did not pay attention to the questionnaire (e.g., some respondents filled out all items with the same answer). After dropping invalid or incomplete responses, only 418 surveys were considered valid. Table 1 shows the detailed demographic information. Since the rating showed no difference, we separated them into high, medium, and low ratings, but we only separated the sample into 4 groups in the experiment. Table 2 shows the number of respondents in each group. The data shows that there are no differences in each group, and the number of valid questionnaires from each groups is greater than 25.

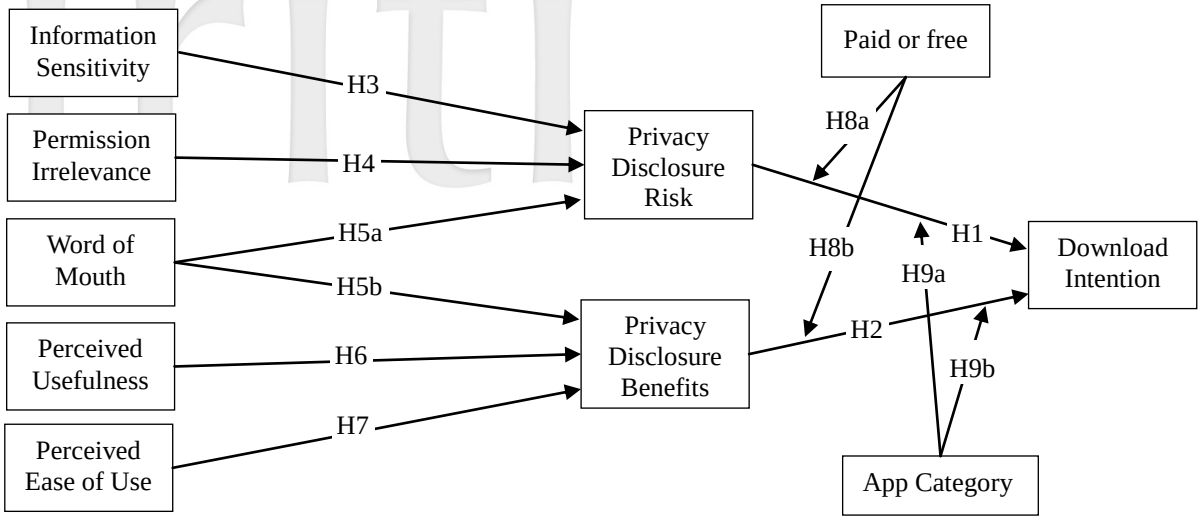

Figure 1 Conceptual Research Model

Source: Summarized by the Authors

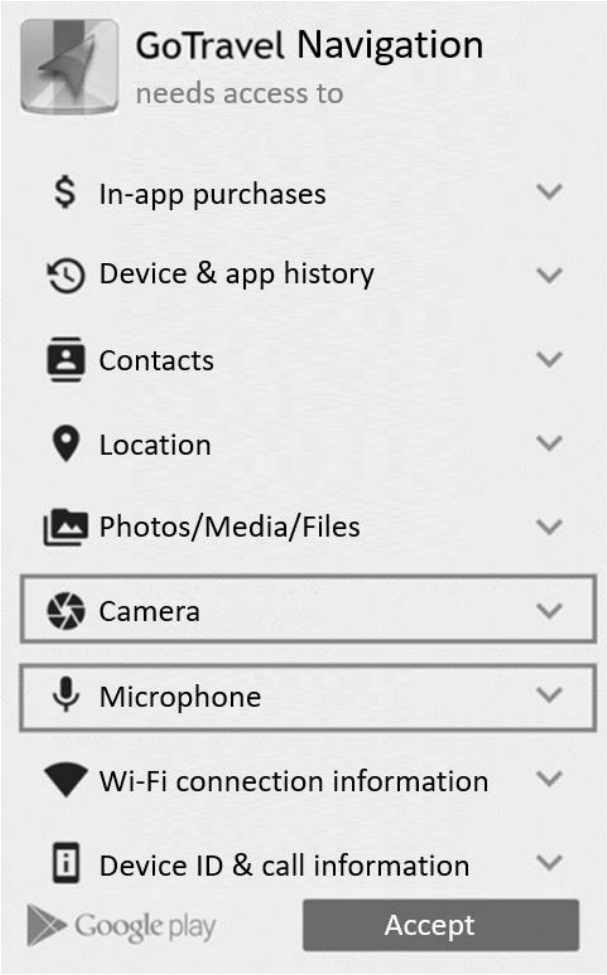

Figure 2 Permissions for the Utilitarian App

Source: Summarized by the Authors

Figure 3 Hedonic App Scenario

Source: Summarized by the Authors

Table 1 Descriptive Statistics of Sample Demographics (N=418)

Measure	Category	Frequency	Percent (%)
Gender	Male	206	49.3
	Female	212	50.7
Age	<20	96	23.0
	21-25	235	56.2
	26-30	33	7.9
	31-35	12	2.9
	36-40	9	2.2
	>41	33	7.9
Degree	Senior high school or under	30	7.2
	University (College)	268	64.1
	Master	108	25.8
	Above Master	12	2.9
Job	Student	282	67.5
	Information industry	50	12.0
	Service industry	41	9.8
	Manufacturing industry	16	3.8
	Financial industry	8	1.9
	Other	21	5.0
Salary	< NT$ 5,000	182	43.5
	NT$ 5,000 - NT$15,000	99	23.7
	NT$ 15,001 - NT$30,000	57	13.6
	NT$ 30,000 - NT$ 45,000	49	11.7
	NT$ 45,001 - NT$60,000	18	4.3
	> NT$ 60,000	13	3.1

Source: Summarized by the Authors

Table 2 Number of Each Group

Group	Free	Pay
Hedonic	Male: 49 Female: 62 (Total: 111)	Male: 49 Female: 52 (Total: 101)
Utilitarian	Male: 59 Female: 50 (Total: 109)	Male: 49 Female: 48 (Total: 97)

Source: Summarized by the Authors

3.2 Measurement Development

In addition to employing privacy calculus theory, we employ a construct development methodology introduced by Xu et al. (2009). As mentioned above, we have added two constructs (paid or free, and app category) into our research model to examine whether or not they affect privacy calculus. Table 3 shows the operational definitions and measurement sources for this study.

Table 3 Operational Definitions

Constructs	Operational definitions	# of items	References
Information Sensitivity	When the personal information attribute, the degree of discomfort an individual perceives when disclosing specific personal information to an LBS app.	3	Dinev et al. (2013)
Permission Irrelevance	Permissions requested by an LBS app which have no relevance to the functions provided by the app	3	Self-developed
WOM-Ratings & Downloads	The ratings and downloads of an LBS app.	3	Self-developed
WOM-Comments	The degree to which users perceive the comments regarding an LBS app to be positive.	4	Ji (2013)
Perceived Usefulness	The user's perception of using a particular LBS app will be of help.	3	Self-developed
Perceived Ease of Use	The user's perception of a particular LBS app will be easy to use.	4	Venkatesh et al. (2003); Zhou (2012)
Privacy Disclosure Risk	The user's perception that disclosing personal information to a LBS app may result in negative results.	4	Dinev et al. (2013)
Privacy Disclosure Benefits	The user's perception of the potential for gaining a positive outcome as a consequence of disclosing personal information to an LBS app.	3	Dinev et al. (2013)
Download Intention	Users' willingness to download an LBS app.	3	Xu et al. (2009)

Source: Summarized by the Authors

3.3 Assessment of Reliability and Validity

We evaluated the reliability, convergent validity and discriminant validity in order to measure the adequacy of our model. Reliability can be examined via composite reliability (CR). CR should be greater than 0.7 (Fornell and Larcker 1981). We can see the results of factor analysis in Table 4, which shows that all the values of all the constructs are between 0.865 and 0.977. Convergent validity is evaluated using factor loadings and average variance extracted (AVE). Fornell and Larcker (1981) noted the standard for convergent validity: the AVE of all constructs should be greater than 0.5. Hair et al. (1998) noted that factor loadings of 0.5 or greater are considered practically significant. Table 4 shows that the AVE of each construct is between 0.689 and 0.924. As shown in Table 4, all factor loadings of

indicator variables are above 0.5. In order to obtain sufficient discriminant validity, the correlation between constructs should be less than 0.90, and the square root of AVE should be greater than the correlation coefficient between constructs. Tables 4 and 5 show that the minimum requirements are met, thereby confirming the quality of our measurements.

4. Result and Discussion

We adopted Smart PLS 2.0 to calculate the β coefficients and significance levels of all the proposed hypotheses. The results including path coefficients and explained variances indicated that some hypotheses are supported as demonstrated in Figure 4. The results show that the relationship between privacy disclosure risks and download intention is negative and significant (β=-0.291, p<0.001). The findings are consistent with the studies of Krasnova, Hildebrand, and Guenther (2009) and Xu et al. (2009). Thus, hypothesis H1 is supported. The relationship between privacy disclosure benefits and download intention is positive and significant (β=0.391, p<0.001). The findings are consistent with the studies of Bellavista, Küpper, and Helal (2008) and Xu and Gupta (2009). Thus, hypothesis H2 is supported. The relationship between information sensitivity and disclosure privacy risks is found to be positive and significant (β=0.196, p<0.01). The findings are consistent with the studies of Jalilvand et al. (2012), Malhotra, Kim, and Agarwal (2004), and Yang and Wang (2009). Thus, H3 is supported. The relationship between permission irrelevance and disclosure privacy risks is also found to be positive and significant (β=0.535, p<0.001). The findings are consistent with the studies of Dinev and Hart (2006), and Zhou (2012). Thus, H4 is supported. Furthermore, the relationship between word-of-mouth (WOM) and privacy disclosure risks is negative and significant (β=-0.106, p<0.05), and the relationship between word-of-mouth (WOM) and disclosure privacy benefits is found to be positive and significant (β=0.221, p<0.001). The findings are consistent with the studies of Albarq (2014), Chong et al. (2018), Jalilvand et al. (2012), and Kim, Kankanhalli, and Lee (2016). Thus, H5a and H5b are supported. In addition, the relationship between perceived usefulness and privacy disclosure benefits is found to be positive and significant (β=0.272, p<0.004). The findings are consistent with the studies of Gefen, Karahanna, and Straub (2003) and Li, Sarathy, and Xu (2010). Thus, H6 is supported. However, though the relationship between perceived ease of use and privacy disclosure benefits is positive, it is not significant. The finding has opposed and inconsistent with the studies of Lee and Benbasat (2004) and Zhang et al. (2010). Thus, H7 is not supported.

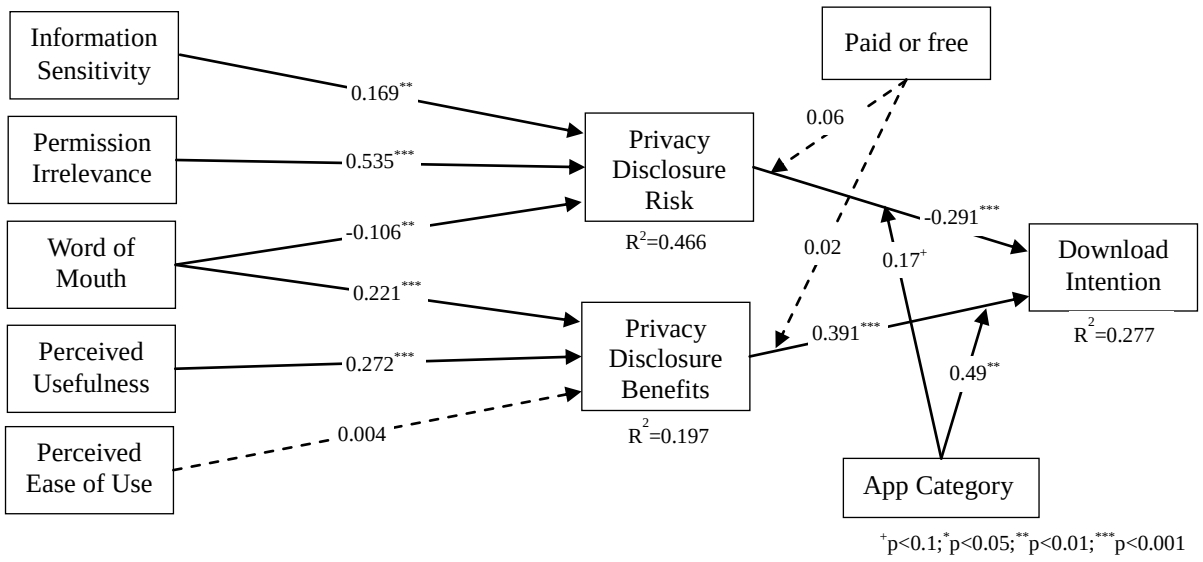

Figure 4 Structure Model and Path Coefficients

Source: Summarized by the Authors

As shown in Figure 4, we were separated the data into paid and free scenarios to test H8. Result shows that neither construct is significant. That means there are no differences between paid and free. The finding has opposed and inconsistent with the studies of Ji (2013) and Metzger (2004). This means that neither H8a nor H8b is supported. Next, we separated the data into utilitarian and hedonic scenarios to test H9. The results are shown though the difference is not significant, there is a difference in the effect of privacy disclosure benefits on download intention. Thus, some users pay more attention to the privacy disclosure benefits when considering utilitarian apps as opposed to hedonic apps. There are also significant differences in the effect of privacy disclosure risks on download intention.

Users are more aware of the privacy disclosure risks regarding hedonic apps. The findings are partially consistent with the studies of Kim et al. (2014) and Xiang et al. (2015). Thus, H9a is supported, but H9b is not supported.

After comparing the two types of app category, we found that users do consider the privacy disclosure risk in both conditions. Unlike the utilitarian condition, users pay more attention to the privacy disclosure risk when the app category is hedonic. That supports our suggestion that users generally focus on the benefits of a utilitarian app. Thus, if the app is considered useful and helpful to the user, although it may involve some privacy risk, the user is still willing to download it. On the other hand, users do not consider hedonic apps to be necessary, so if they have some privacy concerns, they will not want to use the app (e.g., game), and will search for other games instead. That again supports our suggestion that users are more aware of the risks of hedonic apps.

The effect of paid or free is not significant, but when we divided it again by app category we found some differences (see Table 6). In the paid condition, privacy disclosure benefits have an influence in both the hedonic and the utilitarian condition, to a similar degree in each case. This may be because the app costs money, so users are more critical of the app's functions. Privacy disclosure risks also have an influence in both the hedonic and the utilitarian conditions. Nevertheless, the privacy disclosure risks are very significant in the hedonic condition, while in the utilitarian condition, the effect is merely significant.

In the free condition, the privacy disclosure benefits have an influence in both the hedonic and the utilitarian condition (see Table 6). However, users pay more attention to privacy disclosure benefits in the utilitarian condition. Once again, this supports our proposition that users generally focus on the benefits of utilitarian apps. The privacy disclosure risk also has an influence in both conditions, but the impact of privacy disclosure risk is highly significant in the hedonic condition, while it is, again, merely significant in the utilitarian condition.

We found that, in all the above conditions, perceived ease of use does not significantly influence privacy disclosure benefits. May be compared with other business information systems, most of the APP are very easy to use, so it is not the user's concern.

Table 4 The Results of Factor Analysis

Constructs	Items	Loading	ITC
Information Sensitivity (AVE = 0.840, CR = 0.940, Alpha = 0.905)	I'm not comfortable with the type of information the application requires me to provide.	0.913	0.796
	I think this app will collect my highly personal information.	0.927	0.796
	For me, the information provided to this app is very sensitive.	0.909	0.819
Permission Irrelevance (AVE = 0.872, CR = 0.953, Alpha = 0.926)	The permissions of this app are more than needed to fit to its functions.	0.919	0.789
	This app requests too many unnecessary permissions.	0.942	0.861
	The permissions of this app are unreasonable.	0.939	0.814
Word-of-Mouth: Ratings & Downloads (AVE = 0.689, CR =0.865, Alpha =0.756)	There are a plenty of downloads of this app.	0.584	0.324
	The rating of this app is good.	0.921	0.715
	This app is popular.	0.937	0.765
Word-of-Mouth: Comments (AVE =0.873 , CR =0.965 , Alpha = 0.951)	The rating page of this app has many positive ratings.	0.941	0.884
	Most of the comments or opinions of users are positive.	0.943	0.909
	Negative comments of this app are in the lower range.	0.892	0.843
	The positive comments of this app are greater than the negative comments of this app.	0.959	0.920
Perceived Usefulness (AVE = 0.920, CR = 0.972, Alpha = 0.956)	I find this app is useful.	0.948	0.989
	This app can fulfill my needs.	0.967	0.910
	This app is useful for achieving my personal goals.	0.963	0.919
Perceived Ease of Use (AVE = 0.912, CR = 0.977, Alpha = 0.968)	It was easy for me to learn to use LBS.	0.950	0.894
	Skillfully using LBS is easy for me.	0.968	0.911
	I found it easy to learn to use LBS.	0.958	0.890
	For me, using LBS is an easy task.	0.945	0.880
Privacy Disclosure Risks (AVE = 0.760, CR = 0.927, Alpha = 0.894)	It is risky for me to provide personal information to this app.	0.873	0.815
	It seems to me that if I give personal information to this app, there is a real risk of a loss of privacy.	0.934	0.868
	It seems to me that personal information may be improperly used by this app.	0.787	0.705

	For me, providing my personal information to this app involves a lot of unexpected problems.	0.887	0.806
Privacy Disclosure Benefits (AVE = 0.764, CR = 0.907, Alpha = 0.846)	Posting my personal information on this app site will help me get the information/product/service I want.	0.877	0.643
	For me, providing my personal information is the only way I can get what I want from the app.	0.914	0.712
	For me, the disclosure of personal information will benefit me from better, customized services and/or better information and products.	0.830	0.625
Download Intention (AVE =0.880, CR =0.957, Alpha =0.932)	I am willing to download this app.	0.948	0.889
	I am likely to download this app.	0.934	0.879
	I will probably download this app.	0.932	0.879

Source: Summarized by the Authors

Table 5 The Results of Discriminant Validity

Variables	Mean	Std. Dev.	M3	M4	Correlation Matrix								
					Com	PDB	PDR	PR	IS	PEoU	PU	R&D	DI
Com	3.815	1.553	-0.196	-0.695	**0.934**								
PDB	3.792	1.306	-0.015	-0.317	0.383	**0.874**							
PDR	4.997	1.279	-0.318	-0.452	-0.040	-0.218	**0.872**						
PR	4.546	1.386	0.011	-0.525	-0.079	-0.226	0.610	**0.934**					
IS	4.354	1.489	-0.041	-0.619	-0.011	-0.213	0.685	0.723	**0.917**				
PEoU	5.105	1.229	-0.427	-0.005	0.345	0.227	0.268	0.128	0.158	**0.955**			
PU	4.293	1.526	-0.316	-0.457	0.637	0.463	0.049	0.035	0.035	0.582	**0.959**		
R&D	4.051	1.332	0.074	-0.323	0.767	0.390	0.050	-0.007	0.050	0.381	0.619	**0.830**	
DI	3.648	1.572	-0.102	-0.736	0.585	0.533	-0.276	-0.274	-0.255	0.268	0.617	0.520	**0.938**

Note: 1. M3: Skewedness; M4: Kurtosis; The diagonal line of correlation matrix represents the square root of AVE
2. Com: comments; PDB: privacy disclosure benefits; PDR: privacy disclosure risks; PR: Permission Irrelevance; IS: information sensitivity; PEoU: perceived ease of use; PU: perceived usefulness; R&D: rankings & downloads; DI: download intention

Source: Summarized by the Authors

Table 6 The Results of Paid and Free

Path	Paid-Hedonic (n=101)	Paid-Utilitarian (n=97)	Free-Hedonic (n=111)	Free-Utilitarian (n=109)
PDR → DI	-0.456***	-0.166*	-0.343***	-0.188*
PDB → DI	0.423***	0.436***	0.250**	0.548***

Note: 1. DI: download intention; PDB: privacy disclosure benefits; PDR: privacy disclosure risk
2. Numbers in this table reflect the ß coefficient.

Source: Summarized by the Authors

5. Conclusion

5.1 Summary and Implications

This paper was to determine the impact of paid or free and app category on privacy calculus. We also intended to confirm the effects of information sensitivity, permission irrelevance, WOM, perceived usefulness, and perceived ease of use on privacy calculus. We adopted the questionnaire methodology to manipulate different scenarios to present the various paid or free and app category conditions. As a result, our research has two main findings.

First, whether paid or free makes a difference to the user's privacy calculus depends on the app category. In the paid condition, users focus on the privacy disclosure benefits. This means that users will critically consider the app's functionality. Users also attach importance to the privacy disclosure risks of hedonic apps. In the free condition, users attach more importance to the privacy disclosure benefits of utilitarian apps. Second, the app category also impacts the user's privacy calculus. Users focus on the benefits of a utilitarian app and they are more concerned with the risks of a hedonic app.

There are some implications for the researchers from this study. Since there is almost no research discussing the effects of paid or free and app category on privacy risks, our research is the first to provide insight regarding these two constructs in this context. Future studies may use our findings as a reference.

There are some implications for the practitioners from this study. Vendors of hedonic apps must either guarantee the security of their app or explain how the requested permissions are used by the app. Otherwise, the privacy disclosure risks decrease users' intention to download the app. Also, if the app is paid, users focus more on the privacy disclosure benefits, so vendors should make sure the functions of their paid apps are more helpful and meaningful than those of their free apps. Otherwise, users may not want to spend their money on the app. If a free app is utilitarian, users are more concerned with the benefits than they do if the free app is hedonic. Therefore, vendors of utilitarian apps should introduce their app clearly to enhance users' perceptions of the usefulness of it.

5.2 Limitations

Despite our best efforts, this study has some limitations. First, our research focused on users of the Android platform, but the behaviors of IOS platform users might be different. Second, there are many factors that influence privacy calculus, such as device condition and monetary rewards. In order to simplify the conditions, we excluded such factors. Third, in order to simplify the scenarios, we choose only one utilitarian app and one hedonic app to simulate the process of downloading the app for respondents. However, different types of app might make a difference to users. For instance, if the app in the scenarios were used to find restaurants, users who are interested in eating might pay more attention to its benefits. Finally, because of time constraints, this study drew a convenient sample via Facebook, and friends were requested to participate in our survey in Taiwan. Additionally, 67.5% of our respondents were students and 43.5% of our respondents were salary less than $NT5,000. Thus, future research is needed to determine whether these results can be generalized to other age populations.

Reference

Ajzen, Icek and Martin Fishbein (1980), *Understanding Attitudes and Predicting Social Behaviour*. Englewood Cliffs NJ: Prentice Hall.

---- (1991), "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.

Albarq, Abbas N. (2014), "Measuring the Impacts of Online Word-of-Mouth on Tourists' Attitude and Intentions to Visit Jordan: An Empirical Study," *International Business Research*, 7(1), 14-22.

Anderson, Eugene W. (1998), "Customer Satisfaction and Word of Mouth," *Journal of Service Research*, 1(1), 5-17.

Arndt, Johan (1967), "Role of Product-Related Conversations in the Diffusion of a New Product," *Journal of Marketing Research*, 4(3), 291-295.

Barnes, Stuart James (2003), "Known by the Network: The Emergence of Location-Based Mobile Commerce," in *Advances in Mobile Commerce Technologies*, Lim, Ee-Peng and Siau, Keng, ed. Idea Publishing, 171-189.

Beckmann, Svenja (2016), "Exploring the Effects of Type of Permission, Type of Review, and Type of App on People's Risk Perceptions, Trust, Privacy Concerns, and Behavioural Intentions," master thesis, University of Twente, (accessed November 28, 2019), [available at https://essay.utwente.nl/71374/1/Beckmann_MA_BMS.pdf].

Bellavista, Paolo, Axel Küpper, and Sumi Helal (2008), "Location-Based Services: Back to the Future," *IEEE Pervasive Computing*, 7(2), 85-89.

Chau, Patrick Y. K. (1996), "An Empirical Assessment of a Modified Technology Acceptance Model," *Journal of Management Information Systems*, 13(2), 185-204.

Chellappa, Ramnath K. and Raymond G. Sin (2005), "Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management*, 6(2-3), 181-202.

Chen, Liang, Sarang Thombre, Kimmo Järvinen, Elena Simona Lohan, Alén-Savikko Anette, Helena Leppäkoski, M. Zahidul H. Bhuiyan, Shakila Bu-Pasha, Giorgia Nunzia Ferrara, Salomon Honkala, Jenna Lindqvist, Laura Ruotsalainen, Päivi Korpisaari, and Heidi Kuusniemi (2017), "Robustness, Security and Privacy in Location-based Services for Future IoT: A Survey," *IEEE Access*, 5, 8956-8977.

Chong, Isis, Huangyi Ge, Ninghui Li, and Robert W. Proctor (2018), "Influence of Privacy Priming and Security Framing on Mobile App Selection," *Computers & Security*, 78, 143-154.

Clarke, Roger (2001), "Person Location and Person Tracking-Technologies, Risks and Policy Implications," *Information Technology & People*, 14(2), 206-231.

Culnan, Mary J. (1993), "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use," *MIS Quarterly*,17(3), 341-363.

---- and Robert J. Bies (2003), "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues*, 59(2), 323-342.

Cunningham, Scott M. (1967), "The Major Dimensions of Perceived Risk," in *Risk Taking and Information Handling in Consumer Behavior*, Cox F. Donald, ed. Boston: Harvard University Press, MA, 82-111.

Davis, Fred D. (1989), "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly*, 13(3), 319-340.

----, Richard P. Bagozzi, and Paul R. Warshaw (1992), "Extrinsic and Intrinsic Motivation to Use Computers in the Workplace," *Journal of Applied Social Psychology*, 22(14), 1111-1132.

---- (1993), "User Acceptance of Information Technology: System Characteristics, User Perceptions and Behavioral Impacts," *International Journal of Man-Machine Studies*, 38(3), 475-487.

Dinev, Tamara, Heng Xu, Jeff H. Smith, and Paul Hart (2013), "Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts," *European Journal of Information Systems*, 22(3), 295-316.

---- and Paul Hart (2006), "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research*, 17(1), 61-80.

Dowling, Grahame R. and Richard Staelin (1994), "A Model of Perceived Risk and Intended Risk-Handling Activity," *Journal of Consumer Research*, 21(1), 119-134.

Featherman, Mauricio S. and Paul A. Pavlou (2003), "Predicting E-Services Adoption: A Perceived Risk Facets Perspective," *International Journal of Human-Computer Studies*, 59(4), 451-474.

Fornell, Claes and David F. Larcker (1981), "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research*, 18(1), 39-50.

Forsythe, Sandra M. and Bo Shi (2003), "Consumer Patronage and Risk Perceptions in Internet Shopping," *Journal of Business Research*, 56(11), 867-875.

Gefen, David, Elena Karahanna, and Detmar W. Straub (2003), "Trust and TAM in Online Shopping: An Integrated Model," *MIS Quarterly*, 27(1), 51-90.

Hair, Joseph F., Rolph E. Anderson, Ronald L. Tatham, and William C. Black (1998), *Multivariate **Data Analysis:** with Readings*, Englewood Cliffs, NJ: Prentice Hall.

Hann, II-Horn, Kai-Lung Hui, Sang-Yong Tom Lee, and Ivan P. L. Png (2007), "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach," *Journal of Management Information Systems*, 24(2), 13-42.

Harlam, Bari A., Aradhna Krishna, Donald R. Lehmann, and Carl Mela (1995), "Impact of Bundle Type, Price Framing and Familiarity on Purchase Intention for the Bundle," *Journal of Business Research*, 33(1), 57-66.

Hong, Se-Joon and Kar Yan Tam (2006), "Understanding the Adoption of Multipurpose Information Appliances: The Case of Mobile Data Services," *Information Systems Research*, 17(2), 162-179.

Hui, Kai-Lung, Hock Hai Teo, and Sang-Yong Tom Lee (2007), "The Value of Privacy Assurance: An Exploratory Field Experiment," *MIS Quarterly*, 31(1), 19-33.

Jalilvand, Mohammad Reza, Neda Samiei, Behrooz Dini, and Parisa Yaghoubi Manzari (2012), "Examining the Structural Relationships of Electronic Word of Mouth, Destination Image, Tourist Attitude Toward Destination and Travel Intention: An Integrated Approach," *Journal of Destination Marketing & Management*, 1(1-2), 134-143.

Ji, Ya-Pe (2013), "The Effects of Product Information and Social Influence Motivation on Intention to Download Mobile APP Games-The mediating role of Consumption Value," Master Thesis, Department of Business Administration, SooChow University.

Jung, Yoonhyuk, Begona Perez-Mira, and Sonja Wiley-Patton (2009), "Consumer Adoption of Mobile TV: Examining Psychological Flow and Media Content," *Computers in Human Behavior*, 25(1), 123-129.

Junglas, Iris A. and Richard T. Watson (2006), "The U-Constructs: Four Information Drives," *Communications of the Association for Information Systems*, 17(1), 569-592.

---- and ---- (2008), "Location-based Services," *Communications of the ACM*, 51(3), 65-69.

Kaplan, Leon B., George J. Szybillo, and Jacob Jacoby (1974), "Components of Perceived Risk in Product Purchase: A Cross-Validation," *Journal of Applied Psychology*, 59(3), 287-291.

Keith, Mark Jeffrey, Jeffrey S. Babb Jr, Christopher Paul Furner, and Amjad Abdullat (2010), "Privacy Assurance and Network Effects in the Adoption of Location-Based Services: An iPhone Experiment," paper presented at the ICIS 2010 Proceedings, 237, (accessed November 25, 2019), [available at https://aisel.aisnet.org/icis2010_submissions/237/].

Kim, Dongyeon, Kyuhong Park, Yongjin Park, and Jae-Hyeon Ahn (2019), "Willingness to Provide Personal Information: Perspective of Privacy Calculus in IoT Services," *Computers in Human Behavior*, 92, 273-281.

Kim, Gimun, BongSik Shin, and Ho Geun Lee (2009), "Understanding Dynamics Between Initial Trust and Usage Intentions of Mobile Banking," *Information Systems Journal*, 19(3), 283-311.

Kim, Hee-Woong, Atreyi Kankanhalli, and Hyun-Lyung Lee (2016), "Investigating Decision Factors in Mobile Application Purchase: A Mixed-Methods Approach," *Information & Management*, 53(6), 727-739.

----, Hock Chuan Chan, and Sumeet Gupta (2007), "Value-based Adoption of Mobile Internet: An Empirical Investigation," *Decision Support Systems*, 43(1), 111-126.

Kim, Jieun, Yongtae Park, Chulhyun Kim, and Hakyeon Lee (2014), "Mobile Application Service Networks: Apple's App Store," *Service Business*, 8(1), 1-27.

Kim, Jungsun Sunny, Sungsik Yoon, and Dina Marie V. Zemke (2017), "Factors Affecting Customers' Intention to Use of Location-Based Services (LBS) in the Lodging Industry," *Journal of Hospitality and Tourism Technology*, 8(3), 337-356.

Krasnova, Hanna, Thomas Hildebrand, and Oliver Guenther (2009), "Investigating the Value of Privacy in Online Social Networks: Conjoint Analysis," paper presented at the ICIS 2009 Proceedings, 173, (accessed November 25, 2019), [available at https://aisel.aisnet.org/icis2009/173].

Laufer, Robert S. and Maxine Wolfe (1977), "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory," *Journal of Social Issues*, 33(3), 22-42.

Lee, Khai Sheang and Soo Jiuan Tan (2003), "E-retailing Versus Physical Retailing: A Theoretical Model and Empirical Test of Consumer Choice," *Journal of Business Research*, 56(11), 877-885.

Lee, Young Eun and Izak Benbasat (2004), "A framework for the Study of Customer Interface Design for Mobile Commerce," *International Journal of Electronic Commerce*, 8(3), 79-102.

Li, Han, Rathindra Sarathy, and Heng Xu (2010), "Understanding Situational Online Information Disclosure as a Privacy Calculus," *Journal of Computer Information Systems*, 51(1), 62-71.

Liao, Shaoyi, Yuan Pu Shao, Huaiqing Wang, and Ada Chen (1999), "The Adoption of Virtual Banking: An Empirical Study," *International Journal of Information Management*, 19(1), 63-74.

Luarn, Pin and Hsin-Hui Lin (2005), "Toward an Understanding of the Behavioral Intention to Use Mobile Banking," *Computers in Human Behavior*, 21(6), 873-891.

Malhotra, Naresh K., Sung S. Kim, and James Agarwal (2004), "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research*, 15(4), 336-355.

Mallat, Niina, Matti Rossi, Virpi Kristiina Tuunainen, and Anssi Öörni (2008), "An Empirical Investigation of Mobile Ticketing Service Adoption in Public Transportation," *Personal and Ubiquitous Computing*, 12(1), 57-65.

Mazumdar, Tridib and Sung Youl Jun (1992), "Effects of Price Uncertainty on Consumer Purchase Budget and Price Thresholds," *Marketing Letters*, 3(4), 323-329.

McKnight, Harrison D., Nancy Lankton, and John Tripp (2011), "Social Networking Information Disclosure and Continuance Intention: A Disconnect," paper presented at the 44th Hawaii International Conference on System Sciences, (accessed November 25, 2019), [available at https://ieeexplore.ieee.org/document/5718721].

Metzger, Miriam J. (2004), "Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce," *Journal of Computer - Mediated Communication*, 9(4), (accessed November 25, 2019), [available at https://doi.org/10.1111/j.1083-6101.2004.tb00292.x].

Milne, George R. and Mary Ellen Gordon (1993), "Direct Mail Privacy-Efficiency Trade-Offs Within an Implied Social Contract Framework," *Journal of Public Policy & Marketing*, 12(2), 206-215.

Nysveen, Herbjørn, Per E. Pedersen, and Helge Thorbjørnsen (2005), "Intentions to Use Mobile Services: Antecedents and Cross-Service Comparisons," *Journal of the Academy of Marketing Science*, 33(3), 330-346.

Oh, Yuna, Kangsoo Jung, and Seog Park (2014), "A Privacy Preserving Technique to Prevent Sensitive Behavior Exposure in Semantic Location-Based Service," *Procedia Computer Science*, 35, 318-327.

O'Reilly Radar (2011), "Got an iPhone or 3G iPad? Apple is recording your moves," (accessed November 21, 2019), [available at https://cacm.acm.org/opinion/articles/107588-got-an-iphone-or-3g-ipad-apple-is-recording-your-moves/fulltext].

Otjacques, Benoît, Patrik Hitzelberger, and Fernand Feltz (2007), "Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing," *Journal of Management Information Systems*, 23(4), 29-51.

Pagani, Margherita (2004), "Determinants of Adoption of Third Generation Mobile Multimedia Services," *Journal of Interactive Marketing*, 18(3), 46-59.

Palos-Sanchez, Pedro R., José M. Hernandez-Mogollon, and Ana M. Campon-Cerro (2017), "The Behavioral Response to Location Based Services: An Examination of the Influence of Social and Environmental Benefits, and Privacy," *Sustainability*, 9(11), 1988, (accessed November 25, 2019), [available at https://www.mdpi.com/2071-1050/9/11/1988].

Parasuraman, Arun, Leonard L. Berry, and Valarie A. Zeithaml (1991), "Understanding Customer Expectations of Service," *Sloan Management Review*, 32(3), 39-48.

----, Valarie A. Zeithaml, and Leonard L. Berry (1994), "Moving Forward in Service Quality Research: Measuring Different Customer-Expectation Levels, Comparing Alternative Scales, and Examining the Performance-Behavioral Intentions Link," *Marketing Science Institute*, 94-114, (accessed November 25, 2019), [available at http://www.msii.clients.bostonwebdevelopment.com/reports/moving-forward-in-service-quality-research-measuring-different-customer-exp/].

Radner, Roy and Michael Rothschild (1975), "On the Allocation of Effort," *Journal of Economic Theory*, 10(3), 358-376.

Rao, Bharat and Louis Minakakis (2003), "Evolution of Mobile Location-Based Services," *Communications of the ACM*, 46(12), 61-65.

Richins, Marsha L. and Teri Root-Shaffer (1988), "The Role of Involvement and Opinion Leadership in Consumer Word-of-Mouth: An Implicit Model Made Explicit," *Advances in Consumer Research*, 15, 32-36.

Simonin, Bernard L. and Julie A. Ruth (1995), "Bundling as a Strategy for New Product Introduction: Effects on Consumers' Reservation Prices for the Bundle, the New Product, and Its Tie-in," *Journal of Business Research*, 33(3), 219-230.

Stone, Eugene F. and Dianna L. Stone (1990), "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms," *Research in Personnel and Human Resources Management*, 8(3), 349-411.

Strahilevitz, Michal (1999), "The Effects of Product Type and Donation Magnitude on Willingness to Pay More for A Charity-Linked Brand," *Journal of Consumer Psychology*, 8(3), 215-241.

Swan, John E. and Richard L. Oliver (1989), "Postpurchase Communications by Consumers," *Journal of Retailing*, 65(4), 516-533.

Sweeney, Jillian C. and Geoffrey N. Soutar (2001), "Consumer Perceived Value: The Development of a Multiple Item Scale," *Journal of Retailing*, 77(2), 203-220.

Taylor, Shirley and Peter A. Todd (1995), "Understanding Information Technology Usage: A Test of Competing Models," *Information Systems Research*, 6(2), 144-176.

Trepte, Sabine, Michael Scharkow, and Tobias Dienlin (2020), "The Privacy Calculus Contextualized: The Influence of Affordances," *Computers in Human Behavior*, 104, (accessed November 25, 2019), [available at https://doi.org/10.1016/j.chb.2019.08.022].

Venkatesh, Viswanath (1999), "Creation of Favorable User Perceptions: Exploring The Role of Intrinsic Motivation," *MIS Quarterly*, 23(2), 239-260.

---- (2000), "Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model," *Information Systems Research*, 11(4), 342-365.

---- and Fred D. Davis (2000), "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies," *Management Science*, 46(2), 186-204.

----, Michael G. Morris, Gordon B. Davis, and Fred D. Davis (2003), "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly*, 27(3), 425-478.

Wang, Edward Shih-Tse and Ruenn-Lien Lin (2017), "Perceived Quality Factors of Location-Based Apps on Trust, Perceived Privacy Risk, and Continuous Usage Intention," *Behaviour & Information Technology*, 36(1), 2-10.

Wang, Shengling, Qin Hu, Yunchuan Sun, and Jianhui Huang (2018), "Privacy Preservation in Location-Based Services," *IEEE Communications Magazine*, 56(3), 134-140.

Weiner, Bernard (1985), "An Attributional Theory of Achievement Motivation and Emotion," *Psychological Review*, 92(4), 548-573.

Wottrich, Verena M., Eva A. van Reijmersdal, and Edith G. Smit (2018), "The Privacy Trade-off for Mobile App Downloads: The Roles of App Value, Intrusiveness, and Privacy Concerns," *Decision Support Systems*, 106, 44-52.

Xiang, Jun Yong, Lin Bo Jing, Hyun Soo Lee, and II Young Choi (2015), "A Comparative Analysis on the Effects of Perceived Enjoyment and Perceived Risk on Hedonic/Utilitarian Smartphone Applications," *International Journal of Networking and Virtual Organisations*, 15(2-3), 120-135.

Xu, Heng and Sumeet Gupta (2009), "The Effects of Privacy Concerns and Personal Innovativeness On Potential and Experienced Customers' Adoption of Location-Based Services," *Electronic Markets*, 19(2-3), 137-149.

----, Hock-Hai Teo, Bernard C. Y. Tan, and Ritu Agarwal (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.

Yang, Shu and Kanliang Wang (2009), "The Influence of Information Sensitivity Compensation on Privacy Concern and Behavioral Intention," *ACM SIGMIS Database*, 40(1), 38-51.

Yoo, Chul Woo, G. Lawrence Sanders, and Junghoon Moon (2013), "Exploring the Effect of e-WOM Participation on e-Loyalty in e-Commerce," *Decision Support Systems*, 55(3), 669-678.

Zeithaml, Valarie A. (1988), "Consumer Perceptions of Price, Quality, and Value: A Means-End Model and Synthesis of Evidence," *Journal of Marketing*, 52(3), 2-22.

Zhang, Ting, Pei-Luen Patrick Rau, and Gavriel Salvendy (2010), "Exploring Critical Usability Factors for Handsets," *Behaviour & Information Technology*, 29(1), 45-55.

Zhou, Tao (2012), "Examining Location-Based Services Usage from The Perspectives of Unified Theory of Acceptance and Use of Technology and Privacy Risk," *Journal of Electronic Commerce Research*, 13(2), 135-144.

Zimmermann, Andreas, Marcus Specht, and Andreas Lorenz (2005), "Personalization and Context Management," *User Modeling and User-Adapted Interaction*, 15(3-4), 275-302.