Exploring the privacy paradox in mobile app adoption: The roles of an app's aesthetic quality and privacy threats

XI ZHANG

Faculty of Behavioral, Management and Social Sciences

Master: Communication Studies

Specialization: Technical Communication

Student number: s1906445

Supervisor: prof.dr. M.D.T. de Jong

                  dr. Joyce Karreman

Date: 28th August, 2018

UNIVERSITY OF TWENTE.

Abstract

As the mobile app market continue to rapidly evolve, there are many different kinds of mobile apps which could satisfy app users needs in socialization, entertainment and information seeking. However, users often unwittingly disclose their personal information in exchange for mobile services and other benefits, which might impose a threat to app users' privacy. In previous studies, app users' privacy-related decision-making was often seen as a process guided by rationality, in which app users decide to accept a permissions request and share their personal data with a careful assessment between costs and benefits. And most of these research focus on app users' privacy-related behaviors in the Android system. To fill this research gap, this paper proposes and tests a research model of iOS mobile app adoption utilizing the approach of risk-benefit calculation including both rationality and irrationality. It explores the roles of aesthetic quality and privacy threats of a mobile app in affecting perceived benefits, perceived popularity, and perceived privacy risks, and eventually users' download intention. Additionally, it analyzes whether privacy knowledge, privacy awareness and nationality affect app users' privacy-related behaviors.

To answer the research question, a 2x2x2 online experimental study was conducted, with aesthetic quality (good/poor), privacy threats (severe/non-severe), and nationality (Western/Asian) as independent variables. Participants were university students (N=206). Regression analyses revealed that aesthetic quality of mobile app plays an important role in affecting download intention, which is mediated by perceived benefits and perceived popularity. Privacy threats has a relatively weaker significant effect on users' download intention. Asian users had higher download intention than Western users. Meanwhile, female users showed more interests in downloading than male users. However, perceived benefits and perceived popularity had no significant moderation effect on the relationship between privacy threats and download intention. The hypothetical moderation effects of privacy background knowledge and privacy awareness on the relationship between privacy threats and download intention were also be rejected.

The results of research study showed that the influential roles of aesthetic quality, privacy threats, nationality and gender in mobile apps downloading process, and it found the possible reasons of the privacy paradox phenomenon. This study also provided some new insights that can help app users to improve their awareness especially in iOS system. The distinction between Asian and Western app users indicated that the culture difference should be further investigated in the future studies.

Keywords: privacy; privacy paradox; risk-benefit calculation; rationality and irrationality;aesthetic quality; cultural differences

Content

1. Introduction

In recent years, mobile application market has gone through tremendous growth. According to App Annies' report (2017), the worldwide downloads of mobile applications has risen by 60 percent to 175 billion by 2017. Varied mobile applications could satisfy users' needs in several aspects, for example, social networking services, mobile pictures and videos processing, mobile online shopping and etc. However, it should be noted that the usefulness and attractiveness of these mobile applications can also improve potential for privacy invasion to personal information (Robertson, 2016), which may include contact lists, locations, photos and credit card information (Patrick, 2013). As users do not pay for these applications for most of the time, the application developers often reimburse themselves by collecting, using and sharing personal information of users in their unwittingly situation (Gu et al., 2017). And this might impose a threat to users' privacy, because their personal information could be used to transmit to other entities for business aims (Xu, 2012), or to illegal behaviors, such as identity theft (Wottrich et al., 2018) and property loss. Thus, it might be risky when users decide to download an application on mobiles.

In the meantime, users' privacy concerns have also increased with the improvement of application experience and privacy awareness. According to the survey conducted by Boyles, Smith and Madden (2012), more than half of app users have uninstalled or given up installing an app because of their privacy concerns. However, prior research points out that although with privacy concerns, users are still willing to disclose their personal information to apps in order to exchange some benefits, such as retail value, useful information and more personalized services (Sundar et al., 2013). This discrepancy between users' actual behaviors and privacy concerns is a phenomenon, identified as "privacy paradox" (Acquisti, 2004). And multiple studies have investigated this phenomenon in different contexts, such as social network activities, e-commerce and mobile apps (Xu et al., 2010). As one of the most commonly used theories in explaining the discrepancy between privacy concerns and actual technology acceptance behaviors, privacy calculus theory (Dinev & Hart, 2006) believes that users often make rationally trade-off between perceived benefits and perceived risks (Pentina t al., 2016). Moreover, prior research also indicates that decision-making often proceeds in an irrational context rather than in a rational one (Barth & De Jong, 2017). Thus, applying risk-benefit calculation guided by rationality and irrationality research model to understand the users' intentions toward mobile apps download, and finding out the crucial factors which influence the mobile apps adoption could make contribution to the privacy protection and mobile apps businesses development.

In e-tail context, past research has pointed out the importance of attractive and beautiful web designs in promoting users' online navigation and improving users' online shopping experience (Ganesh et al., 2010). Although some research tried to figure out the reciprocity of perceived benefits and perceived risks driving users'

decision to download mobile apps, no research takes the design of mobile apps as a potential factor in the trade-off between benefits and risks in mobile download context. Thus, aesthetic quality was included as the predictor in our research.

Furthermore, each application in mobile device could ask users' permission to access certain resources, and this permission-based security model is different between Android and iOS system. For Android system, users accept the permissions during the installation process (Barrera et al., 2010). In iOS system, mobile apps request users' permission after downloading. Many papers examined consumers reaction to app permission requests in the app download stage, especially in Android system. However, no extant research focuses on the privacy policies which include permission requests which mobile apps provide in iOS system. Privacy policies often inform consumers about items of information collection, how information will be used and who can access to their information,which could refer to privacy threats information. But few app users pay attention to these important information. This study focuses on the mobile apps download stage for two reasons. Firstly, different from personal computers and other devices, mobile phones *can facilitate data collection and sharing among many entities, including application developers, analytic companies, and advertisers to a degree unprecedented in the desktop environment* (FTC, 2013). Secondly, *the download stage can be the first layer of defense against privacy-invasive apps* (Gu et al., 2017).

Based on risk-benefit calculation research model, this study examines the effects of aesthetic quality and privacy threats to users' download intention towards a video-making mobile app. In addition, the important role that culture plays in technology acceptance has been investigated by several existing studies (Straub, Keil, &Brenner, 1997; Pentina et al., 2016). By conducting online experiment among Asian and Western students in University of Twente, this study also aims to make a cultural comparison between Asians and Westerns. To fill in the gap of the literature to date, this study aims to shed lights on the potential roles of aesthetic quality and privacy threat in the apps download decision-making. Thus, this study seeks to answer the following research question:

> *How do aesthetic quality and privacy threats of apps influence users' app download intention among Western and Asian users?*

This study has contributed to both scientific and practical perspectives. Scientifically, this research is the first to study the joint effects of aesthetic quality, privacy threats and nationality on personal users' downloading intention. Practically, this study offers meaningful insights for app developers into understanding the app download decision-making process of consumers in different countries, and then constantly improve their apps. Moreover, it can strengthen consumers' awareness of privacy policy in the download stage.

2. Theoretical Background and Research model

2.1 Privacy Paradox in iOS Download Stage

As the information technology becomes indispensable in daily life, consumers are accustomed to download various mobile apps to satisfy their needs. And in this process, consumers often unknowingly disclose their personal information, such as contact lists, photo albums, credit cards and device ID to exchange for the mobile apps services. However, their unwittingly leakage of private information may lead to privacy invasion. Recently, a growing number of literature has focused on privacy problems in Andriod System because of its huge market share, open source OS, also its permission request in the download stage, which makes it become vulnerable to privacy-invasive apps (Felt et al., 2012). However, there has been minimal research focused on iOS system. Although in iOS Appstore, *"all applications must pass through a vetting process (performed by Apple in a closed manner) before reaching consumers"* (Barrera et al., 2010), the application developers could still get privacy information through collecting customers' personal information, and may share these data with third parties. Moreover, most iOS app users ignore the privacy policies which include these important privacy-related information in the Appstore. Thus it is interesting to study their download intention in iOS system.

Recent literature points out that the users' decision to apply mobile applications is mainly determined by attractiveness, usability and popularity (Li, Sarathy, & Xu, 2010; Kelley et al., 2013), in spite of the potential of privacy invasion and leakage. However, prior studies also indicated that the consumers are concerned about their privacy (Balebako et al., 2011). Thus, this difference between privacy attitudes and actual behavior is known as the "privacy paradox" phenomenon: *"users claim to be very concerned about their privacy but do very little to protect their personal data."* (Barth & De Jong, 2017). The fact is that users' risks perception expresses their knowledge of privacy protection strategies, but they do not have enough motivators to apply such strategies (Oomen & Leenes, 2008). Hence, even though users show great concerns to privacy issues and hold a positive attitude to privacy protective behaviors, they rarely take actual behaviors accordingly (Joinson et al., 2010). Some scholars explain why users with privacy risks awareness are still willing to share private information on Internet. The main reason is that they tend to exchange their personal information for more customized services (Magedanz & Simoes, 2009) or retail value (Acquisti & Grossklags, 2005). For example, in the context of SNS use, Facebook users disclose large amounts of sensitive personal information including name, address, phone number and pictures (Tufekci, 2008) to maintain their social relationships and manage their social impressions, even while being aware of the risks the SNS may pose to their personal data (Taddicken, 2014). In the attempts to investigate and explain privacy paradox, a prior study has developed an theoretical framework to address the discrepancy between actual behavior and privacy concerns

in the mobile application context (Barth & De Jong, 2017). They believe that users' decision-making process is mainly driven by two considerations: (a) risk-benefit evaluation guided by rationality and (b) risk assessment guided by irrationality. As this research presents a systematic review of all the studies related to privacy paradox in the context of mobile applications, it is interesting to do further research based on this theoretical model.

2.2 Risk-Benefit Calculation Guided by Rationality

In the context of mobile applications, the risk-benefit calculation plays an important role in decision-making. It represents the freedom of determining to what extent personal information is shared (Li et al., 2010). Users rationally weigh benefits and risks to make decisions of information disclosure. Their intention and actual behaviors are positively related to expected benefits, but negatively affected by possible costs. In addition, the perceived benefits often exceed perceived risks, which accounts for the ignoring of privacy concern that often leads to the private information exposure in exchange for the social, economic, leisure, information quality and convenience benefits (Culnan & Armstrong, 1999; Chua, Goh, & Lee, 2012). Users also pay more attention to the actual benefits they could get rather than to the privacy concerns they previously stated (Poikela et al., 2015). According to *Rational Ignorance Theory* (Downs, 1957), individuals tend to neglect information when they believe that their effort to understand information (costs) are disproportionate to the perceived potential benefits. In mobile application context, users are unwilling to read and understand the complex privacy policies (costs of cognitive effort and time), since they consider that the benefits of using service outweighs the potential danger of privacy invasion (Flender & Müller, 2012). There are several theories which could be applied in users' decision process within privacy calculation, which indicate that information disclosure is guided by rational cost-benefit calculations where benefits outweigh risks. We decide to use the privacy calculus theory, a most commonly used theory in rational decision-making process, as our theoretical framework.

2.2.1 Privacy Calculus Theory

As the most commonly used framework to study privacy perceptions, privacy calculus theory could be regarded as a rational theory that tries to explain the attitudes, beliefs and behavioral intention of Internet users. Privacy calculus theory (PCT) addresses joint effects of opposing forces, for example, perceived benefits and risks on privacy perceptions and behaviors (Laufer & Wolfe, 1977; Li, 2012). The decision of disclosing information is based on *Expectancy theory*, which states that people try to maximize the positive and minimize negative outcomes (Vroom, 1964). And according to Laufer and Wolfe (1977), individuals tend to disclose their information in exchange for some benefits in the case of their personal information will be used reasonably and without bad consequences in the future. They can also accept privacy

invasion to some extent, as long as they can assure they will get certain benefits through this process and the level of risks is bearable.

Dinev and Hart (2006) investigated this concept, using PCT to study the behavior of individuals on Internet. Subsequently, many studies have been extending PCT to examine user's mobile app download and acceptance intention. When considering to download an mobile application, customers may experience an ambivalence. On the one hand, they are attracted by expected benefits, for example, product attractiveness and usefulness (Li, Sarathy, & Xu, 2010). On the other hand, they may realize the potential privacy risks that might come with downloading process. That is to say, app users can have contrary beliefs about benefits and costs of disclosing information at the same time (Dinev & Hart, 2006). At last, individuals' behavior is decided by the result of a context-specific trade-off between benefits and costs weighs (Jiang et al., 2013; Xu et al., 2011). The privacy calculus model has been used in several studies. For example, in the contexts of e-commerce and location-based services, individuals' adoption of the app is driven by the assessment of the value of mobile apps. And the benefits such as personalized services and compensations positively influenced information disclosure and download intention (Yang & Wang, 2009; Xu et al., 2009), while privacy concerns were negatively affecting the extent of adoption of these online services.

2.2.2 Perceived App Benefits

Privacy calculus theory states that perceived benefits could counteract perceived risks in individual's decision process. The definition of benefits in PCT is broad, for example, Morton (2014) classified benefits with tangibles (cash payments, cheaper products and services) and intangibles (recommendations, social benefits and etc). Some studies illustrate that benefits related to information disclosure include economic advantages (Li, Sarathy, & Xu, 2010), social benefits (Lu, Tan, & Hui, 2004) , entertainment and information seeking (Lin, Fang, & Hsu, 2014).

Considering how many benefits a mobile app could offer, individuals might be more or less inclined to download this app. When app users get to know a new app, the attractiveness of this app might be the most important dimension which influence app users' benefit perception and download intention. App users may evaluate app attractiveness in line with usefulness (Li, Sarathy, & Xu, 2010) and design (Patrick, Lorrie, & Norman, 2013). In addition, according to Technology Acceptance Model (TAM), perceived usefulness and perceived ease of use (Davis, 1989) are two predictors to adopt a new technology. Also, this TAM theory has been extended to study the individual' s behavior of privacy-related problems (Pavlou, 2001). Thus, in the context of mobile app, perceived usefulness refers to the extent which the app user believes that using mobile app can help them create videos, and it could be regarded as one of the foremost factor that determine app users' benefit perception and download intention (Gefen, Karahanna, & Straub, 2000). And for perceived ease if

use, it refers to *"the degree to which a person believes that using a particular system would be free of effort"* (Radner & Rothschild, 1975). Thus, the mobile apps should be easier to use than others similar product, and they will be more likely to be accepted by app users. Besides these two factors, benefit perception could also be driven by aesthetically design of the app according to a survey (Patrick, Lorrie, & Norman, 2013). Recent research has proved that app users' acceptance of the apps is positively influenced by perceived app benefits (Pentina et al., 2016; Gu et al., 2017). Thus, we can expect that:

   H1. *Perceived benefits are positively related to app users' download intention.*

2.2.3 Perceived App Popularity

Perceived app popularity is also an important dimension to determine download intention. When users have to make decision of downloading an app, they often seek for related information. First, they typically rely on their own past experiences in these kinds of products. However, when they do not have any experience with a specific product, they often rely on the experiences of other customers of same product, which expressed as online reviews (Gu et al., 2017). The number of reviews can reflect the reliability of the general opinion of this product. In this sense, app reviews can be the indicator of app popularity. And according to prior research, perceived app popularity is the signal of app benefits. It represents not only the quantity of prior app users, but also the product attractiveness and quality (Duan, Gu, & Winston, 2009). Users tend to download an app which is perceived as popular, because they believe that earlier adopters should have evaluated the quality of app carefully, which will increase the benefits they get from the app. Hence, we can expect that:

   H2. *Perceived popularity is positively related to app users' download intention.*

2.2.4 Perceived App Privacy Risks

The perceived privacy risks, according to Featherman and Pavlou (2003), refers to the *"degree to which an individual believes that a high potential for loss is associated with the release of personal information to a firm"*. And they also pointed out that one of the important facets of perceived risks is the opportunistic behavior by mobile developers, which may result in potential loss of personal information. Mobile apps downloaded on individual's mobiles may detect users' device ID, location and some sensitive information. And these personal information could be sold to the third parties (advertisers, government agencies, financial institutions and etc.) to get misused, which may lead to security problems. Thus, it is reasonable that a user would be reluctantly adopt and use new apps if they believe there is a possibility of information intrusion by mobile app developers (Xu et al., 2011). Several research

have also demonstrated that perceived app privacy risks negatively affects intention to download and use new apps (Keith et al., 2013), which is also consistent with *Expectancy theory* that customers are tend to minimize negative consequences. Hence, we can hypothesize that:

H3. *Perceived privacy risks are negatively related to app users' download intention.*

The correlation model based on privacy calculus theory can be depicted as follows:
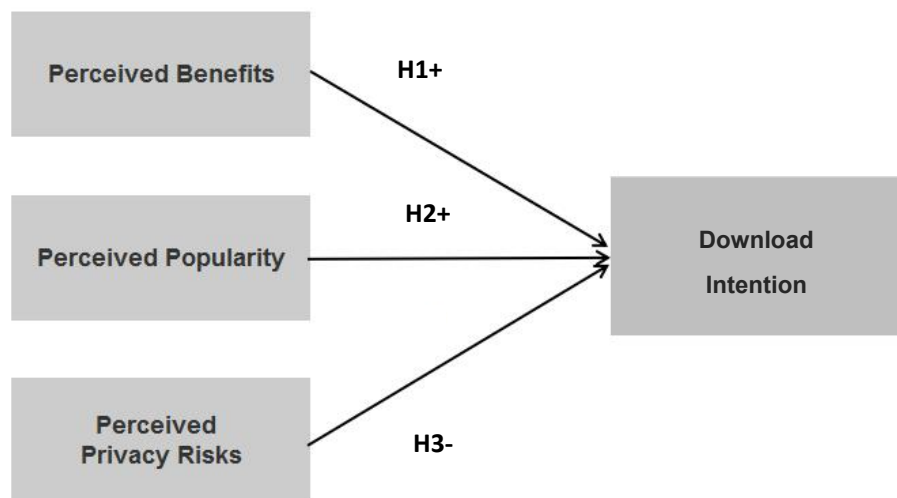
Figure 1. Privacy Calculus Model

2.3 Risk-Benefit Calculus Guided by Irrationality

Contrary to the rational risk-benefits calculation, the different kinds of biases could affect users' decision-making process, such as heuristics, situation cues, under-(over) estimation of the risks and benefits, (immediate) gratifications, risk diffusion, time constrains and so on (Barth & De Jong, 2017). In addition, the *bounded rationality* theory believes that individuals could hardly be rational in decision-making because of the limits of cognitive ability and enough time (Simon, 1982). Thus, all these factors will result in subconscious biases in the risk-benefit calculations. Hence, it is inevitable that users usually make decisions rapidly without a comprehensive and rational analysis.

According to *Optimistic Bias Theory* (Irwin, 1953), individuals have a tendency to underestimate experiencing negative events, which could lead to unawareness of the threat and reluctant behaviors of privacy protection (Acquisti, 2004). Also, the

Immediate Gratification Theory (O' Donoghue & Rabin, 2001) indicates that individuals often encounter self-control issues because of (immediate) gratification, which may result in negative outcomes over the long term. In this condition, users with general privacy concerns could make decisions to disclose their private information in return for the immediate benefits in the short term. Several studies point out that users usually discount the probability to encounter privacy risks, and immediate gratification could weaken privacy concerns leading to poor privacy protection behavior (Acquisti, 2004; Acquisti & Grossklags, 2005; Deuker, 2010).

2.4 Research Model

In the above section, we proposed that risk-benefits calculation guided by both rationality and irrationality have affected users' decision-making process. In the mobile app download context, we want to investigate the effect of aesthetic quality and privacy threats on users' download intention, which is driven by rational and irrational risk-benefit analysis. As privacy background knowledge, privacy awareness and nationality also played important roles in influencing mobile app users' behavior in prior research, we also include them in the models to investigate their effects.

Mobile App Aesthetic Quality

Mobile apps with high- aesthetically quality will indirectly increase users' tendency to have a deeper inquiry into their hedonic needs (Wang et al. 2011). And app user's download intention can be determined by the quality of a mobile app (Hassenzahl, 2004). However, it is difficult for users to understand a mobile apps' usefulness and quality through short-time browsing in Appstore. Thus, when app users are not finding any specific apps, attractiveness can be regarded as an important factor in quality assessment and download intention (Vassileva, 2012). According to Lavie and Tractinsky (2004), the attractiveness perception from individuals is often generated in aesthetics through design factors like creativity and harmony. They has categorized aesthetics into two dimension, namely classical aesthetics and expressive aesthetics. The classic aesthetics is represented with well-organized and symmetrically balanced interface. And the expressive aesthetics includes the dimensions related to creativity, originality and fascinating elements. To make an aesthetically designed interface, it requires of the balance of both dimensions. The mobile app interface is usually served as a mediation between the system and user involvement, interactivity and information communication. An aesthetically beautiful interface can create positive visual experience, catch the individual's attention, and it can also have immense effect on individual's emotion (Bhandari et al., 2017; Wang et al. 2011). As a factor in user interface design, aesthetic quality has huge impacts on usability issues in HCI (Human Computer Interaction), and it also has positive effect on the individuals' perception towards the mobile app quality evaluation (Tuch, 2010; Zhang & Adipat, 2005). Moreover, prior research pointed out that individuals will be more satisfied

when service is offered with aesthetically designed interface (Iris & Anat, 2006). Thus, app users will become more interested and confident in app quality and usefulness, which will contribute to their download intention. Hence, we can expect that:

H4. *The aesthetic quality of an app is positively related to app users' download intention.*

As mentioned above, the attractiveness of the mobile apps is driven by aesthetic quality, and it often has a positively effect on users' perception towards the mobile apps quality evaluation. Thus, a high-aesthetically designed interface could easily impress users with usefulness and ease of use, which will contribute to users' benefit perception. Moreover, according to earlier studies, the perceived benefits has positively effect on users' download intention. Since little research found direct relationships between aesthetic quality and download intention, we propose a mediator model in which the perceived benefit was treated as a mediator variable. The aesthetic quality (independent variable) influences the mediator variable, which in turn influences users' download intention (dependent variable).

Hence, we can expect that:

H5. *The effect of aesthetic quality on download intention is mediated by perceived benefits.*

Moreover, earlier studies indicate that users' satisfaction often comes from highly attractive and beautiful interface designs, regardless the usefulness of the websites (Lindgaard & Dudek, 2013). Van der Heijden (2003) also pointed out that the aesthetic appeal of a website is positively associated with users' pleasure. The high-aesthetically mobile app interface could enhance users' enjoyment and contribute to their assessment on mobile apps' quality, which could also perform positive influences on their perception about mobile app popularity. Since perceived popularity has a positively effect on download intention, as well as the mediation analysis mentioned above, we can hypothesize that:

H6. *The effect of aesthetic quality on download intention is mediated by perceived popularity.*

Privacy Threats

Privacy threats can be defined as the possible privacy issues caused by organizations, such as over-collection of personal information, improper access to personal information, misuse of personal information, unauthorized access and theft, share personal information to third parties (Rindfleisch, 1997; Smith et al., 1996). And privacy concern can be defined as individual's concern about privacy threats. If individuals find that the privacy threats are high, their privacy concern about privacy

threats can be considered as the main obstruction when accepting a new technology. Dinev and Hart (2006) firstly applied privacy concern in the PCT model as the privacy cost, and they believed that privacy concern about privacy threats is negatively related to the information disclosure on the Internet. Other research also pointed out that privacy concern have negative impacts on willingness to disclose personal information to create personal profiles (Culnan & Amstrong, 1999), intentions to accept the permission request when download mobile apps (Mark, Samuel, & Joanne,2012), and online purchase (Metzger, 2004; Smith, Dinev & Xu, 2011). In addition, prior research has shown that IT users may behave differently when they experience privacy threats, and their different levels of privacy concern may effect their responses toward the mobile apps. If users perceive high level privacy threats, they would have a low intention to accept a new system. For the mobile download stage, we can expect that:

H7. *The privacy threats of an app are negatively related to app users' download intention.*

According to PCT and Keith et al. (2013), individuals conduct a risk-benefit analysis that leads to their behavioral decisions in face of privacy threats, and app users' privacy concern about privacy threats of apps will increase their situational and context-specific perceived privacy risks. Thus, based on these research, it is assumed that individual with high levels of privacy concern about privacy threats are related to a higher level of perceived privacy risks. And based on the mediation model, the privacy threats (independent variable) influence perceived privacy risks (mediator variable), which affect users' download intention (dependent variable) at last.

H8. *Privacy threats' effect on download intention is mediated by perceived risks.*

Based on the theoretical background, the experimental research models (Figure2) is developed to depict how users' download intention is affected by assessment of aesthetic quality and privacy threats.
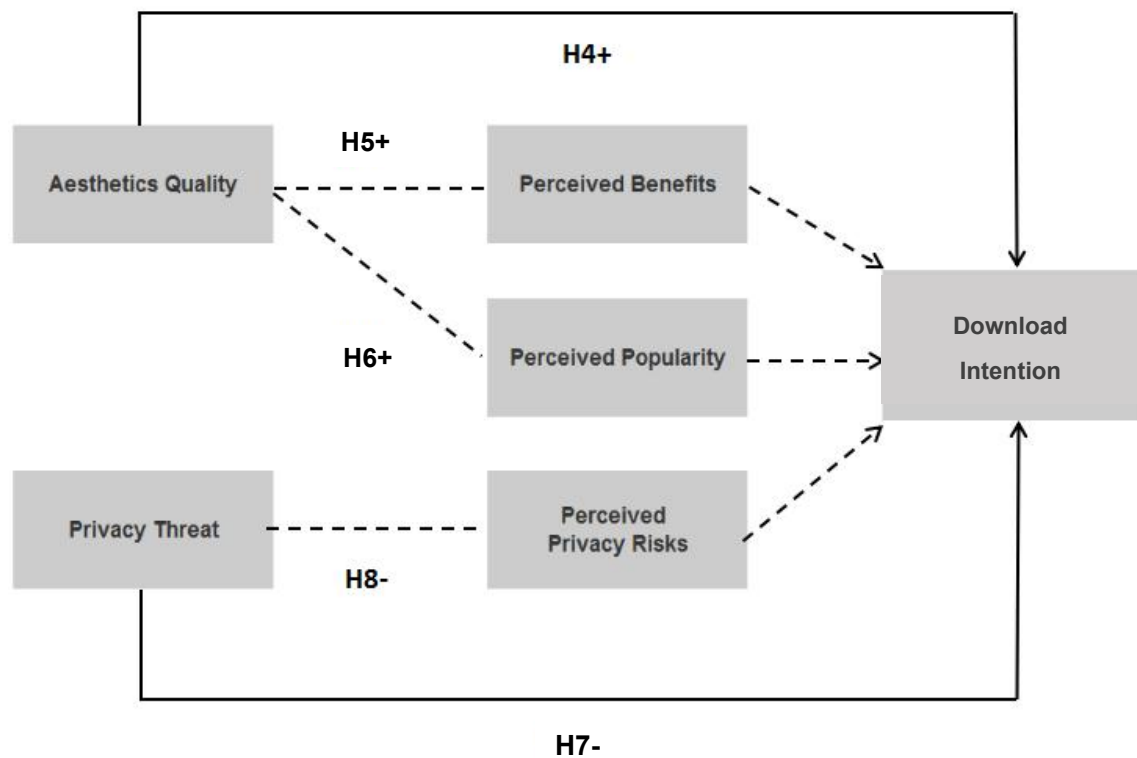
Figure 2. Overall Experimental Research Model

Positive and negative effect ⟶   *Mediation effect* - - ➤

Possible Irrational Elements in Decision-making Process

Under the irrational risk-benefit calculation process, individuals can be easily influenced by different kinds of biases. As mentioned above, users are inclined to underestimate their own privacy risks due to the (immediate) gratification. Users' tendency to get immediate benefits (e.g. using an app to make a video), which will lead to poor privacy protection behaviors by ignoring privacy risks perception. Therefore, the aesthetic quality of mobile app may alter the strength of the relationship between perceived privacy risks and download intention.

Then we can expect that:

> **H9.** *Aesthetic quality positively moderates the effect of perceived risks on users' mobile app download intention.*

Moreover, according to the biased decision-making process, perceived benefits and perceived popularity can also be considered as immediate gratification, since they

14

both have positive correlations to users' download intention according to prior research. Individuals are inclined to neglect their privacy concern, discounting the low probability of future privacy risks (e.g. leakage and misuse of personal information), which leads to a propensity to immediate benefits (e.g.the instantaneous use of a beautiful and popular mobile app). Thus, perceived benefits and perceive popularity may have a weaken effect on privacy threats to perceived risks for download decision. In this model, the perceived benefits and perceived popularity can be considered as the moderators that affects the strength of the relation between privacy threat to download intention, as well as their mediation relationship accordingly (See Figure3).

Hence, we can expect that:

H10a. *Perceived benefits positively moderate the effect of privacy threats on download intention.*

H10b. *Perceived benefits positively moderate the effect of privacy threats on perceived risks.*

H10c. *Perceived benefits positively moderate the effect of perceived risks on download intention.*

H11a. *Perceived popularity positively moderates the effect of privacy threats on download intention.*

H11b. *Perceived popularity positively moderates the effect of privacy threats on perceived risks.*

H11c. *Perceived popularity positively moderates the effect of perceived risks on download intention.*
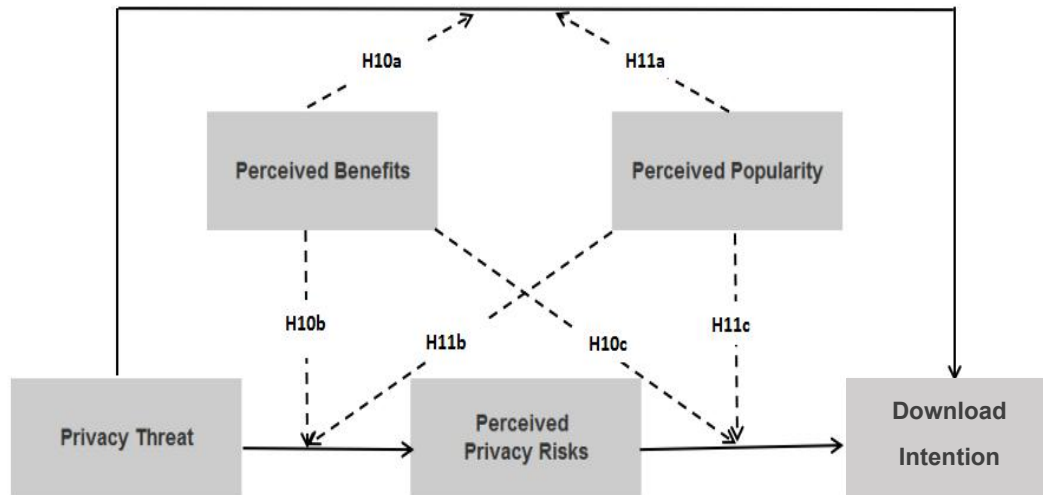
Figure3. Moderation Model of relation between privacy threats and download intention

Positive and negative effect ——→   *Moderation effect* - - -→

Roles of Privacy Background Knowledge and Privacy Awareness

The prior research has recognized privacy background knowledge and privacy awareness as critical factors of privacy-related behaviors. For example, an earlier study found that individuals who have higher levels of privacy background knowledge and privacy awareness pay more attentions to the information safety, which results in lower intention to disclose personal information online. Hence, we expect that these two factors may have effect on users' download intention. Also, we hypothesize that users who have knowledge and awareness of privacy are more concern about privacy risks in the specific mobile app download context (Modaresnezhad et al., 2013; Awad & Krishna, 2006).

Roles of Culture Difference between Asian and Western Users

According to Hofstede (1984) and prior research, culture can be defined as the collective programming of the mind which distinguishes one human group from another. For example, Asian and Western users may have reverse tendencies toward a new technology because of "*self-direction (way of thinking and innovatory), conformity (restraining from actions that may violate expectations or norms), and security (placing a high priority on harmony and stability of group)*" (Pentina et al., 2016). Users in low uncertainty avoidance cultures, like USA, they would have more willingness to adopt a new technology, while users in high uncertainty avoidance cultures would think a lot about uncertain situations and restrict their willingness to

accept the new technology, such as Chinese users(Hofstede, 1991). Thus, it is interesting to include users from different cultures to study their download intention to the mobile apps.

In addition, several prior research have been investigating and comparing the difference of app adopting and using behaviors between different cultures. For example, Iryna and Li (2016) have found that US users paid more attentions to the perceived app benefits, and they are not interested in new apps as Chinese users. Also, according to the prior survey, it is normal that users tend to accept information-sensitive mobile apps in China, while things are different in US (Yang, Lu, Gupta, & Cao, 2012). In m-commerce context, Dai and Palvia (2009) pointed out that American and Chinese m-commerce users were similar in their perception of privacy, perceived usefulness and ease of use. But the American users enjoyment perception are higher while Chinese users' concern for costs of e-commerce is higher. Meso, Musa, and Mbarika (2005) found that culture differences had a significant effect on perceived benefits of mobile apps. According to Cao and Everard's research (2008), the culture differences had huge impacts on users' privacy concern and awareness, resulting in their different intention toward the instant messaging on mobiles. Thus, it is reasonable that culture could affect individuals' personal traits, which may affect their perception of benefits and risks, as well as their adopting behaviors. The important role of culture plays in mobile apps contexts has been empirically proved by the research mentioned above. Thus, we expect that mobile app users from Asian and Western cultures would have conduct different risk-benefit calculations, which lead to different download intention.

3. Methodology

3.1 Design

To study the download intention regarding the aesthetic quality and privacy threats of mobile apps between different cultures, we designed a prototype of a video-making mobile app named "Vshot" in iOS system to be evaluated by research participants. The experimental design was a 2 (aesthetic quality: high aesthetic quality vs.low-aesthetic quality) × 2 (privacy threats: low risks vs. high risks) × 2 (nationality: Asians vs. Westerns) factorial design. Aesthetic quality, privacy threats and nationality are the independent variables, perceived app benefits, perceived privacy risks, perceived popularity and users' download intention are the dependent variables. To measure the variables, we conducted an online experiment designed in English as this is the dominant language at university among all the students. Qualtrics was applied to design the questionnaire owing to its professional functions and advanced compatibility across different devices.

3.2 Stimulus Materials

To increase the validity and develop the stimulus material for the final experiment, we conducted a pre-test among 50 students in University Twente at first stage. In this pre-test, participants were randomly and equally given one of the two versions of Vshot prototypes in Appstore, and they evaluated this mobile app from aesthetics quality. Since everyone has different aesthetics criteria, we want to make sure the prototypes we made conform to the mass aesthetic appreciation level. Based on the result, it was significantly that users indicated one version as a high-aesthetically designed interface, which meets our expectation. Hence, we developed and revised the five prototype pages for each version in Appstore which include both aesthetics design and privacy information for final experiment.

The four different versions which were used as stimulus materials are shown in Appendix 1. These prototype pages fully imitated the information pages in Appstore, containing the details about aesthetics app interface and privacy policy. From first three prototype pages, users can get visual information of the Vshot from its logo, interface details including color, font and layout. Users could also have an impression of the functions and reviews of Vshot. In the version of high aesthetic quality, the design of app is in visual clarity, and the colors, fonts and layout are creative and consistent. On the contrary, the low-aesthetics app featured a messy and rigid layout with discrepant colors and font. As for the latter two prototype pages, we collected and analyzed more than 20 video-making apps' privacy policy, and forming two different versions of privacy policies. One is low privacy risks version which collects reasonable personal information (e.g. username, Email and necessary registration information) and use these information in a proper way. The other one is high privacy

risks version with several privacy problems including over-collecting personal information (e.g. registration information, phone number, billing information, home address), unauthorized use and access, sharing and selling personal information with third parties.

3.3 Measures

The measurement scales of the experiment based on reviewing literature, and were adapted to the research context. The experimental questionnaire is shown in Appendix 2.

Perceived benefits. Perceived benefits were measured on a five-point scale ranging from 1, "disagree," to 5, "agree." adopted from the research of Davis (1989) and Xu et al. (2010), including 8 items. Example items include "I think Vshot looks as if it is well-designed." and "I think Vshot will help me create excellent videos."

Perceived popularity. Perceived popularity was measured on a five-point scale, including 4 items. Example items include "I think Vshot is popular among users." and "I think Vshot has a high rating." After factor analysis, we deleted one item.

Perceived privacy risks. It was measured by the items derived from Dinev (2006),Xu et al. (2011) and Mark (2012), comprising 8 items. All items were measured by 5-point scales. As privacy threats include over-collection, unauthorized access and misuse of personal information (Rindfleisch,1997; Smith et al., 1996). Example items include "I think downloading and using Vshot may threaten my personal privacy." and "I would be concerned that Vshot may misuse my personal information." After factor analysis, we removed one item.

Download intention. Including 7 items, users' download intention was measured on a five-point scale and also a one-item scale adopted from Bernritter et al.(2016). Participants indicated their download intention of this new app by moving a 100-point (0 to 100%) slider. The higher the percentage, the more willingness participants were to download the "Vshot" on mobile phone. Example items include "I would be willing to download Vshot on my mobile phone." and " If I want to edit a video on my mobile phone, I would be inclined to try Vshot." After factor analysis, we removed one item.

Privacy background knowledge. It was measured on a five-point scale, including 3 items. Example items include "I am aware of the privacy risks of mobile apps." and "I know how mobile apps may invade the privacy of users."

Privacy awareness. Including 4 items, privacy awareness was measured on a five-point scale. It was based on the *global information privacy concern* items developed from Malhotra et al. (2004). Example items include "I think it is important to protect my privacy." and " I am really concerned about potential privacy threats."

3.4 Procedure

When participants read the introduction page of the questionnaire and consent to continue, they were randomly and roughly evenly assigned to one of the four conditions (2 levels of aesthetics × 2 levels of privacy) by Qualtrics website randomizer function. Next, they were asked to carefully read the information on each of the screens (five in total), which including both aesthetically designed interfaces and privacy information. Then, participants were asked to fill a questionnaire in which they need to judge the "Vshot" from several aspects, such as overall impression, willingness to download, quality of Vshot, expected popularity, privacy aspects. Hereafter, participants answered the background information which includes knowledge and awareness about privacy, as well as demographics. Lastly, they were thanked at the end of the questionnaire. The whole process takes about 5-10 minutes.

3.5 Participants

We chose college students because they are familiar with mobile apps, and they fit well with the video-editing app we designed. This experiment also involved both Asian and Western students in University of Twente to study whether different cultures have different impact on the trade-offs between mobile app aesthetic quality and privacy threats. We post the web link through several channels to recruit participants, such as Emails, Facebook, Whatsapp groups, and other social medias. A total of 326 students in University of Twente participated in the experiment voluntarily. After removing responses that were incomplete, and finished in short time (less than 240 seconds), the final participants number was 206. All these participants were roughly evenly assigned to four different versions, with at least 50 participants in each version. Among the 206 respondents, there were 82 males (40%) and 124 females (60%), 115 Asians and 91 Westerns. The average age of respondents was 24, and there were 104 Bachelors, 92 Masters and 10 PhDs. Chi-square tests and ANOVA showed that age, and educational levels and nationality did not differ significantly across the four different Vshot versions. However, it revealed that gender showed significant correlation to nationality (See Appendix 3). ANOVA also indicated that gender had impact on download intention. Thus, we believe that our random assignment process was not effective enough, and in further analysis we included gender as a predictor.

4. Results

4.1 Scale Construction

Before testing the hypotheses, we conducted a exploratory factor analysis (EFA) to assess the convergent and discriminant validity of the constructs (See Appendix 4). When measuring perceived benefits, perceived privacy risks and perceived popularity in mobile apps using context, all items were subjected to a principle component factor analysis with Varimax rotation (Costello & Osborne, 2005). We found that all the factor loading were above the cutoff value of 0.5, with no cross-loading of 0.4 or above. However, we found that one of the items measuring perceived popularity and one of the items measuring perceived privacy risks had a result factor loading lower than 0.4. After removing these two item, we can say all the constructs conform the criteria for validity.

Moreover, we checked reliability using Cronbach alphas (α). As shown in Appendix 4, all the values ranged from 0.91 to 0.94, exceeding the recommended threshold of 0.7 (Nunnally, 1978).

4.2 Relations between Intermediate Variables and Download Intention

Conducting hierarchical regression analysis (See Table 4.2), we found the relations between intermediate variables (nationality, gender, privacy knowledge, privacy awareness, perceived benefits, perceived popularity and perceived privacy risks) and download intention.

The result indicated that the perceived benefits had positively effect on download intention (β=.70, p<.05), supporting H1. Hypothesis 2 was supported because perceived popularity positively correlated with download intention (β=.17, p < .01).In contrast, perceived privacy risks showed no significant correlation relationship to Vshot download intention, thus H3 is rejected.

Table 4.2 *Results hierarchical regression analysis*

	Model 1	Model 2
Nationality	-.16*	-.10*
Gender	.14*	.02
Privacy knowledge	.04	-.07
Privacy awareness	.24**	-.01
Perceived benefits		.70***
Perceived popularity		.17**
Perceived privacy risks		.02
Adjusted R^2	.13***	.68***

Note: * p<.05, ** p<.01, *** p<.001

4.3 Direct and Mediated Effects of Aesthetic Quality and Privacy Threats on Download Intention

The ANOVA of General Linear model in SPSS was used to test the direct effects of aesthetic quality and privacy threats on download intention between Asian and Western users. According to the result (See in Table 4.3.1), the app users' download intention was significantly affected by aesthetic quality, supporting Hypothesis 4. The privacy threats also had an effect on download intention, thus H7 is confirmed. In addition, nationality and gender were also significantly related to users' download intention.

Based on the result of main and interaction effects on download intention shown in *Table 4.3.2*, we found that high aesthetic quality mobile app leads to high download intention (M=3.9, SE=0.99), while low aesthetic quality mobile app resulted in lower download intention (M=3.3, SE=0.79). Furthermore, users' download intention was higher when mobile apps had low privacy threats (M=3.7, SE=.09). In contrast, users' download intention was lower when the privacy threats were high (M=3.4, SE=.08). Asian users (M=3.8, SE=.08) have higher download intention than Western users (M=3.4, SE=.09), while female (M=3.7, SE=.07) tend to have higher download intention than male (M=3.4, SE=.09).

Furthermore, result indicated that the interaction between privacy threats and gender, as well as gender and nationality were significantly related to download intention. Based on the result, it could be seen that in the low privacy threats condition, the mobile app download intention of male (M=3.8, SE=.14) and female (M=3.8, SE=.11) were both higher than in the high privacy threats condition. However, in the high privacy threats condition, females (M=3.8, SE=.11) tend to have higher download intention than males (M=3.1, SE=.12). In the interaction relationship of gender and

nationality, we found that Asian females (M=4.0, SE=.09) had significantly higher download intention than Western females (M=3.4, SE=.12), while Asian and Western males had similar download intention.

Table 4.3.1 *Mean scores and standard deviation for the significant main and interaction effects*

	df	F	Sig.
Aesthetic quality	1,190	24.882	.000***
Privacy threats	1,190	5.719	.018*
Gender	1,190	5.404	.021*
Nationality	1,190	9.298	.003**
Aesthetic quality * Privacy threats	1,190	.001	.981
Aesthetic quality * Gender	1,190	2.666	.104
Aesthetic quality *Nationality	1,190	3.266	.072
Privacy threats * Gender	1,190	10.075	.002**
Privacy threats * Nationality	1,190	.170	.681
Gender * Nationality	1,190	5.275	.023*
Aesthetic quality*Privacy threats*Gender	1,190	.052	.819
Aesthetic quality * Privacy threats * Nationality	1,190	.064	.800
Aesthetic quality*Gender*Nationality	1,190	3.420	.066
Privacy threats*Gender*Nationality	1,190	1.885	.171
Aesthetic quality * Privacy threats * Gender * Nationality	1,190	.069	.793

*p < .05. **p < .01. ***p < .001

Table 4.3.2 *Mean scores and standard error for the significant main and interaction effects*

	Download intention	
	Mean	**Std. Error**
Aesthetic quality		
Low	3.3	.08
High	3.9	.08
Privacy threats		
High	3.4	.08
Low	3.7	.09
Nationality		
Asians	3.8	.08
Westerns	3.4	.09
Gender		
Male	3.4	.09
Female	3.7	.07
Interaction privacy threats * gender		
Low threats & Male	3.8	.14
High threats & Male	3.1	.12
Low threats & Female	3.8	.11
High threats & Female	3.7	.11
Interaction nationality * gender		
Asian & Male	3.5	.14
Asian & Female	4.0	.09
Western & Male	3.4	.12
Western & Female	3.4	.12

Note: Measured on a five-point scale (1 = low intention, 5 = high intention).

And the mediation analysis based on Baron and Kenny (1986) was conducted to assess if the mediators mediate the relationship between independent variable and dependent variable. First, we tested the effect of independent variable and dependent variable. Second, we examined if the independent variable affected the mediators. Last, we regressed the dependent variable against the independent variable and mediators. This section discusses the results of these analyses, and the result was shown in Table 4.3.3.

H5, H6, H8 were tested with the aesthetic quality and privacy threats were treated as independent variables and download intention to Vshot was treated as the dependent variables, while perceived benefits, perceived popularity and perceived privacy risks were regarded as mediators. For the mediation analysis, we found that aesthetic quality positively affected users' download intention (β=0.25, p<.001), and aesthetic quality significantly predicted the perceived benefits (β=0.34,p<.001), also the

relationship between perceived benefits (mediator) and download intention was significant (β=.20, p<.01). When include both aesthetic quality and perceived benefits, we found that perceived benefit remains significant. Thus, the effect of aesthetic quality on download intention is completely mediated by perceived benefits, confirming H5. Furthermore, we found the relationship between aesthetic quality and perceived popularity was significant (β=.20, p<.01), and perceived popularity had effect on download intention (β=.12, p<.05). After involving both aesthetic quality and perceived popularity, perceived popularity still have effect on download intention (β=.11, p<.05). Thus, the perceived popularity was proved to have mediation effect on aesthetic quality and download intention, H6 is supporting. In contrast, result showed no significant mediation effect of perceived privacy risks toward privacy threats and download intention, which rejects H8.

Table 4.3.3 Mediating Analysis

Relationship	β	Adjusted R Square
Aesthetic Quality→Download Intention	.25***	.06
Aesthetic Quality→Perceived Benefits	.34***	.11
Perceived Benefits→Download Intention	.82***	.67
Aesthetic Quality+Perceived Benefits→ Download Intention		
Aesthetic Quality	-.03	.67
Perceived Benefits	.83***	.67
Aesthetic Quality→Download Intention	.25***	.06
Aesthetic Quality→Perceived Popularity	.20**	.04
Perceived Popularity→Download Intention	.12*	.67
Aesthetic Quality +Perceived Popularity →Download Intention		
Aesthetic Quality	-.03	.67
Perceived Popularity	.11*	.67
Privacy Threats→Download Intention	-.08*	.00
Privacy Threats→Perceived Privacy Risks	-.11	.01
Perceived Privacy Risks→Download Intention	.04	-.00
Privacy Threats+Perceived Privacy Risks→Download Intention		
Privacy Threats	.05	.00
Perceived Privacy Risks	.08	.00

*p < .05. **p < .01. ***p < .001

4.4 Effects of Aesthetics-related Variables On the Relationship Between Privacy Threats to Download Intention

In order to test Hypothesis 9 to Hypothesis 15, we used PROCESS v3.1 (Hayes,2017), a an observed variable OLS and logistic regression path analysis modeling tool for SPSS to investigate the interactions and conditional indirect effects in moderated mediation models,using a single or multiple moderators (Hayes, 2012). We applied Model 1 of PROCESS for probing the moderation analysis. And the result was shown in Appendix 5.

According to the result, the moderating effect of aesthetic quality on the relationship to perceived privacy risks to download intention was not significant, rejecting Hypothesis 9. Perceived benefits had no significant moderating effect with privacy threats on download intention, rejecting Hypothesis 10. Not in line with Hypothesis 11, perceived popularity showed no relatively significant moderating effect with privacy threats on download intention. Following the moderation testing procedure of PROCESS, we found that the moderating effects of perceived benefits and perceived popularity on the relationship between privacy threats and perceived privacy risks were not significant. Hence, Hypothesis 12 and Hypothesis 13 were not supported, The results also showed that perceived benefits and perceived popularity showed no significant moderating effect on perceived privacy risks to download intention. Thus, Hypothesis 14 and Hypothesis 15 were rejected. All in all, we found no significant moderation effect of perceived benefits and perceived popularity on the relationship between privacy threats and download intention.

4.5 Effects of Privacy Background Knowledge and Privacy Awareness

Using PROCESS model, we also investigated the effects of privacy background knowledge and privacy awareness on the relationship between privacy threats and download intention (See Appendix 6).

According to the result, we found that the privacy background knowledge had no significant moderation effect on the relationship between privacy threats to download intention. Also, the result indicated that it had no moderation effect on the relationship between privacy threats to perceived privacy risks, as well as the relationship between perceived privacy risks to download intention.

Meanwhile, privacy awareness showed no significant moderation effect on the relationship between privacy threats and download intention. And it also had no significant moderation effect on the relationships between privacy threats to perceived privacy risks and perceived risks to download intention. Thus, we can conclude that these two factors have no effect on users' download intention.

5.Discussion and Implication

5.1 Main Findings

This study applied the rational and irrational risk-benefit calculation framework to test research models examining the roles of aesthetic quality and privacy threats in affecting users' app download intention among Asian and Western mobile app users. From our research result (See Table 5.1), we found that the perceived benefits and perceived popularity are positively related to download intention, while perceived privacy risks showed no significant correlation to download intention. For the experimental model, we found that aesthetic quality has a significant main effect on download intention, which is mediated by perceived benefits and perceived popularity. Privacy threats have a relatively weaker effect on download intention, however perceived privacy risks have no mediation effect to the relationship between privacy threats to download intention.

Meanwhile, we also found nationality and gender are significantly related to download intention. Asian users have more interests in downloading Vshot, while western users' download intention is lower. Gender also plays an important role in users' decision process. Female users have higher download intention than male users, especially in high privacy threats version. In addition, Asian females showed significantly higher download intention to Vshot than Western female users.

Based on moderation analysis, we found that neither perceived benefits nor perceived popularity showed significant moderation effects on the relationship between privacy threats and download intention. Similarly, privacy background knowledge and privacy awareness have no significant moderation effect on the relationship between privacy threats and download intention.

Table 5.1 *Summary of the hypotheses testing results.*

	Results
H1. Perceived Benefits (PB)→Download Intention (+)	Supported
H2. Perceived Popularity (POP)→Download Intention (+)	Supported
H3. Perceived Privacy Risks (PPR)→Download Intention (-)	Rejected
H4. Aesthetic Quality→Download Intention	Supported
H5. Aesthetic Quality→Perceived Benefits→Download Intention	Supported
H6. Aesthetic Quality→Perceived Popularity→Download Intention	Supported
H7. Privacy Threats→Download Intention	Supported
H8. Privacy Threats→Perceived Privacy Risks→Download Intention	Rejected
H9. Aesthetic Quality→Download Intention moderated by PPR	Rejected
H10a. Privacy Threats→Download Intention moderated by PB	Rejected
H10b. Privacy Threats→Perceived Privacy Risks moderated by PB	Rejected
H10c. Perceived Privacy Risks→Download Intention moderated by PB	Rejected
H11a.Privacy Threats→Download Intention moderated by POP	Rejected
H11b. Privacy Threats→Perceived Privacy Risks moderated by POP	Rejected
H11c. Privacy Threats→Perceived Privacy Risks moderated by POP	Rejected

5.2 Theoretical Contributions

This research sheds light on risk-benefit calculation of mobile apps and offers theoretical contributions. First, there are many research using privacy calculus theory to study users' behavior to mobile apps. For example, Wottrich et al. (2018) investigated the roles of app value, intrusiveness and privacy concerns using privacy calculus theory. Pentina et al. (2016) did a culture comparison between US and China to explore users' adoption of information-sensitive mobile apps based on privacy calculus theory. These studies discuss the possible roles to influence app users download behavior based on rational benefit-risk calculation. However, these research neglected the irrational risk-benefits calculation process. In our study, we formed two research models to investigate both risk-benefit calculation guided by rationality and irrationality, and including several possible irrational elements to affect users' download intention, which contribute to find the possible reasons for the privacy paradox phenomenon.

The participants did both rational and irrational risk-benefit calculation in decision-making process, however, we believe that their decision to download Vshot occurs in irrational situation rather than on a rational one. Because in high privacy threats version, females still expressed high download intention than males, which implies that female mobile app users may not conduct a careful assessment between risks and benefits in decision-making process. The reason that female users have higher download intention might due to females could be easily attracted by benefits (e.g. aesthetic quality) than males (Gu et al., 2017). And their belief of the benefits

gained from downloading mobile apps behavior exceeds the risks (e.g. privacy concerns), and the perceived risks could be discounted for short-term benefits(e.g. app use), which in line with earlier research (Alessandro & Jens, 2005; Alessandro, Curtis, & Liad, 2016). When individuals' perceptions of obtained benefits is high and strong, their risk perception does not have enough effect on their actual behavior to avoid risks (Norberg & Horne, 2007). In addition, the reasons could be that mobile app users make their decision without evaluating potential privacy risks, or they have considered but were restricted by the ability to process the huge amount of privacy policies to develop a privacy rational, sensitive and protective decision. According to Vila's research (2004), 41% individuals who claim to have high privacy concerns admit that they rarely read privacy policies.

Moreover, Asian and Western app users have different decision in downloading process. Asian people have higher download intention than Western people. The reasons could be that western app users are more cautious when they tend to download a new app on their mobile phone, which in line with the research conducted by Pentina et al.(2016).

Secondly, prior research often regard the usefulness, ease of use, social or entertainment of mobile app as benefits predictors. For example, Nikkhah and Sabherwal (2017) included perceived usefulness and perceived ease of use in perceived benefits based on TAM in mobile cloud-computing apps. Li, Xu and Sarathy (2010) treat monetary rewards and perceived usefulness as perceived benefits in mobile e-commerce contexts. And these research explored the effects of these factors to app users' download intention mediated by perceived benefits. But they do not contemplate the aesthetic quality. Actually, when individual's aesthetics perception of a mobile app is positive, their benefits perceptions will improve correspondingly, which will also have positive influences on users' download intention.

Thirdly, this research is the first to study the joint effects of app aesthetic quality, privacy threats and nationality on app users' download intention, which sheds more light on the privacy paradox phenomenon. Although nationality has been included in earlier research models, it was often regarded as a control variable with no significant influence. However, our findings support that the difference of nationality indeed influence the mobile app download intention.

5.3 Practical Implications

In addition, this study provides practical implications for app developers, app users and Appstore. Since app developers and Appstore need to make profits on app downloads, it is necessary for them to know about app users' trade-offs in downloading stage. Firstly, since aesthetic quality has significantly positive effect on download intention, app developers should pay more attention on app design,

especially for the information pages in Appstore, which should conforms both classic and expressive aesthetics dimensions.

Secondly, the reason of privacy threats' weaker effect on download intention might due to that mobile app users' restriction ability to process large amounts of privacy information including in privacy policies, their unawareness of privacy risks or their lacking of privacy protection knowledge (Barth & De Jong, 2017). Thus it is important for app developers to explain the purpose of personal data collection and protection practices to app users in a more effective way. Also, it is important for Appstore to regulate the app developers of privacy collection and use.

Thirdly, from a user's perspective, we suggest that individual users should pay more attention and understand privacy information of the mobile apps. Our findings implies that although app users state to have high privacy awareness and background knowledge, they tend to download apps without considering about privacy risks. The ignorance of privacy invasion may lead to "*a herding consequence that the diffusion of privacy-invasive app is hard to stop*" (Gu et al., 2017).

5.4 Limitations and Suggestions for Future Research

The study has several limitations that provide opportunities for future research.

First, our research models are based on both rational and irrational risk-benefit calculation theory to investigate users' download intention. However, download intention is not the actual and final behavior, and initial intention could not represent users' long term intention and disclosure behaviors. Thus, the future research could also integrate more behavior theories. For example, the prospect theory (Kahneman & Tversky, 1979) and social exchange theory (Blau, 1964). The theory states that people make decisions based on the potential value of losses and gains, and they might take account of current potential risks when they make decision in new risks context. Also, losses are more heavily calculated than an equal amount of gains. As for social exchange theory, it explains the roles of risk and benefit in exchange relationship, not with isolated effect. Thus, these two theories could contribute to the study of long-term private information disclosure behavior. The mobile app uses may consider more about long-term investment, rather than the immediate and short-term benefits. In addition, future research could also involve participants in a longitudinal experiments with actual mobile apps rather than prototypes of interface to investigate and measure their actual behaviors of downloading.

Another limitation of this study is its focus on the general level of aesthetics appreciation. However, when individuals evaluate the aesthetics of a product, they usually think from different dimensions. For example, the shape, font, color, layout, style and symmetry (Lavie & Tractinsky, 2004). Although we proved the importance

of the aesthetics in app design and users' download intention, the exact factors to influence aesthetics assessment remain vague. Thus, performing experiment with different aesthetics dimension to find the determining factor of users' evaluation could be a useful future research direction.

Concerning our experimental design, it is possible that users skipped the privacy information pages, as they had no patience to read the whole privacy policies to understand the information. Thus, future research should apply some methods to guarantee the duration of reading information.

Finally, our experiment was only based on university students, which is likely biased towards the groups of highly-educated people rather than all app users. Hence, it is necessary to perform experiments among older and less-educated people in future research.

5.5 Conclusions

Mobile privacy has already became an increasingly significant problems nowadays. As app download behavior is the first stage of app users' privacy consideration, it is crucial to investigate and understand users' decision-making in this process. This study is the first to examine the potential roles of aesthetic quality and privacy threats in iOS mobile apps download decision-making among Asian and Western users. Through the experiment, we apply the risk-benefit calculation research models and find the value of aesthetic quality and privacy threats in the privacy trade-offs and download intention. In addition, several different attitudes toward mobile apps between Asian and Western app users result in their different download behaviors. Based on our findings, we suggest that app users should pay more attention to the privacy policies in Appstore, and develop their rational privacy protective attitude to protect their own personal information. In addition, it is also necessary to increase the regulation of privacy intrusion of mobile apps, restricting the over-collection and unauthorized sharing activities of app developers.

References

Acquisti, A., & Grossklags, J. (2004). Privacy attitudes and privacy behavior. *Economics of Information Security. Springer, US,* 165-178.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy, 3*(1), 26-33.

Andrew F. Hayes.(2017). Introduction to mediation, moderation, and conditional process analysis: A regression-based approach. London: Guilford Publications.

Awad, N.F.,Krishnan,M.S.(2006).The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization, *MIS Quarterly 30* (1) ,13-28.

Balebako, R., Leon, P. G., Almuhimedi, H., Kelley, P. G., Mugan, J., Acquisti, A., .Sadeh, N. (2011). Nudging users towards privacy on mobile devices. Paper presented at the CEUR Workshop Proceedings.

Barrera, D., Kayacik, H.G., Van Oorschot, P.C., & Somayaji, A. (2010). A methodology for empirical analysis of permission-based security models and its application to Android, Proceedings of the 17th ACM Conference on Computer and Communications Security, 73-84.

Barth, S., & De Jong, M. D. T. (2017). The privacy paradox - Investigating discrepancies between expressed privacy concerns and actual online behavior - A systematic literature review. Telematics and Informatics, 34(7), 1038-1058.

Baron, R. M., and D. A. Kenny. (1986). The moderator mediator variable distinction in social psychological research: conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology 51* (6), 1173-1182.

Bernritter, S. F., Verlegh, P. W. J., & Smit, E. G. (2016). Why nonprofits are easier to endorse on social media: the roles of warmth and brand symbolism. *Journal of Interactive Marketing, 33*, 27-42.

Bhandari, U., Neben, T., Chang, K., & Chua, W. Y. (2017). Effects of interface design factors on affective responses and quality evaluations in mobile applications. *Computers in Human Behavior,* 72, 525-534.

Boyles, J. L., Smith, A., & Madden, M. (2012). Privacy and data management on mobile devices. http://www.privacylives.com/wp-content/uploads/2012/09/PIP_MobilePrivacyManagement-092012.pdf.

Cao, J., & Everard, A. (2008). User attitude towards instant messaging: The effect of espoused national cultural values on awareness and privacy. *Journal of Global Information Technology Management, 11*(2), 30-57.

Chua, A. Y., Goh, D. H. L., & Lee, C. S. (2012). Mobile content contribution and retrieval: An exploratory study using the uses and gratifications paradigm. *Information Processing & Management, 48*(1), 13-22.

Costello, A. B., & Osborne, J. W. (2005). Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis. *Practical Assessment Research, and Evaluation, 10*, 1-9.

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

Dienlin, T., & Metzger, M. J. (2016). An extended privacy Calculus model for SNSs: analyzing self-disclosure and self-withdrawal in a representative U.S. sample. *Journal of Computer-Mediated Communication, 21*(5), 368-383.

Dinev, T., & Hart,P. (2006). An extended privacy calculus model for E-commerce transactions. *Information Systems Research,17*(1), 61-80.

Downs, A., (1957). An economic theory of political action in a democracy. J. *Political Economy,65* (2), 135-150.

Duan, W., Gu, B., & Whinston, A. B. (2009). Informational cascades and software adoption on the Internet: An empirical investigation. *MIS Quarterly: Management Information Systems, 33*(1), 23-48.

Fang, J., Li, J., & Wang, R. (2017). Mobile travel apps' adoption: Integrating perceived characteristics of innovation and software quality. Paper presented at the ACM International Conference Proceeding Series.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-Services Adoption: A Perceived Risk Facets Perspective. *International Journal of Human-Computer Studies,59*(4), 451-474.

Federal Trade Commission (FTC), (2013). Mobile privacy disclosures: building trust through transparencyRetrieved from www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf

Felt, AP., Chin, E., Hanna, S., Song, D., & Wanger, D. (2011). Android permissions demystified, Proceedings of the 18th ACM Conference on Computer and Communications Security, 627-638 (Chicago, IL, USA. October 17-21).

Flender, C., & Müller, G. (2012) Type indeterminacy in privacy decisions: The privacy paradox revisited. In: *Vol. 7620 LNCS. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (pp. 148-159).

Felt, A. P., Chin, E., Hanna, S., Song, D., & Wagner, D. (2011). Android permissions demystified. Paper presented at the Proceedings of the ACM Conference on Computer and Communications Security.

Gefen, D., Karahanna, E., and Straub, D., (2003). Trust and TAM in online shopping: an integrated model, *MIS Quarterly, 27*(1), 51-90.

Gu, J., Xu, Y. C., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems, 94*,19-28.

Hamilton, J. D., & Wall, K. D. (1982). Models of bounded rationality in decision making. I*EEE Circuits and Syst Soc, New York, NY, USA.*

Hassenzahl, M. (2004). The interplay of beauty, goodness, and usability in interactive products. *Human-Computer Interaction, 19*(4), 319-349.

Indratmo, & Vassileva, J. (2012). The role of social interaction filter and visualization in casual browsing. Paper presented at the Proceedings of the Annual Hawaii International Conference on System Sciences.

Irwin, F.W. (1953). Stated expectations as functions of probability and desirability of outcomes. *J. Pers. 21* (3), 329-335.

Jiang, Z., Heng, C. S., & Choi, B. C. F. (2013). Research Note-Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. *Information Systems Research, 24*(3), 579-595.

Joshua, F., & Elham, N. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior,25,*153-160.
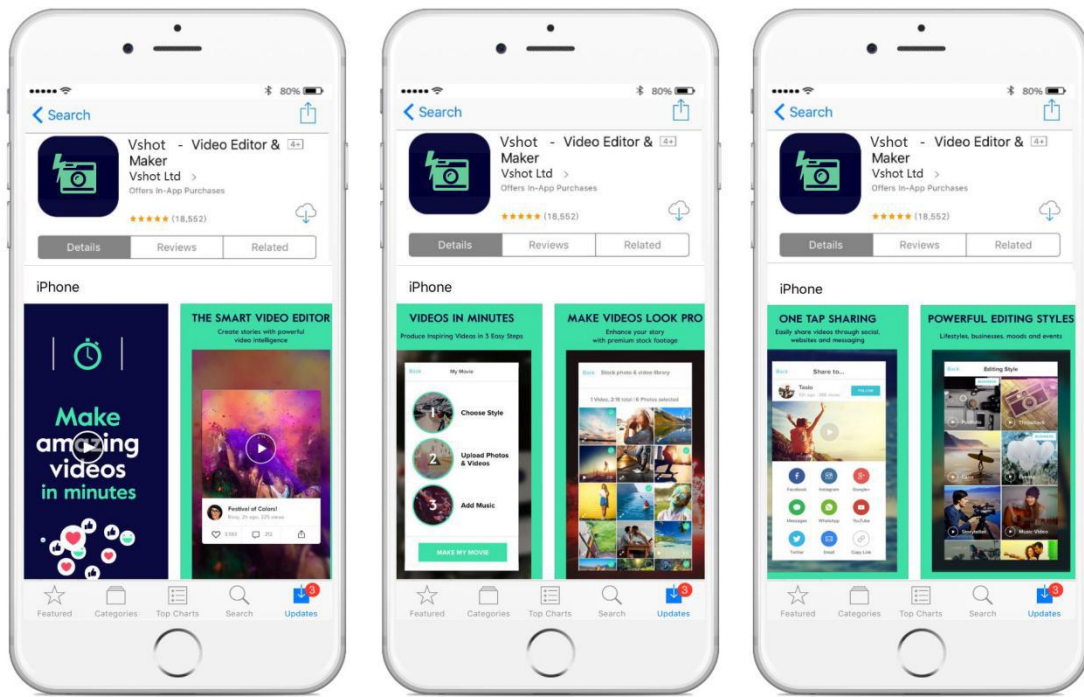
Junglas, I.A., Johnson, N.A., Spitzmüller, C. (2008). Personality traits and concern for privacy: An empirical study in the context of location-based services, *European Journal of Information Systems, 17* (4),387-402.

Kahneman, D., & Tversky, A. (1979). Prospect theory: an analysis of decision under risk. *Econometric, 47*, 263-291.

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.

Laufer, R.S., & Wolfe, M. (1977). Privacy as a concept and a social issue: a multi-dimensional developmental theory. *Journal of Social, 33*, 22-42.

Lavie, T., & Noam T. (2004). Assessing dimensions of perceived visual aesthetics of web sites, *International Journal of Human-Computer Studies, 60* (3), 269-98.

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, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems 51*(3), 434-445.

Lin, Y. H., Fang, C. H., & Hsu, C. L. (2014) Determining uses and gratifications for mobile phone apps. In*: Vol. 309 LNEE. Lecture Notes in Electrical Engineering* (pp. 661-668).

Lu, Y., Tan, B., & Hui, K-L. (2004). Inducing Customers to Disclose Personal Information to Internet Businesses with Social Adjustment Benefits, ICIS 2004 Proceedings, 45. http://aisel.aisnet.org/icis2004/45.

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*, 336-355.

Magedanz, T., & Sim~oes, J. (2009). What happens when you mix social networks, contexts and mobile advertising in the same glass? *International Journal of Mobile Marketing, 4*(2), 52-60.

Meso, P., Musa, P., & Mbarika, V. (2005). Towards a model of consumer use of mobile information and communication technology in LDCs: The case of sub-Saharan Africa. *Information Systems Journal, 15*(2), 119-146

Nikkhah, H. R., & Sabherwal, R. (2017). Mobile cloud-computing applications: A privacy cost-benefit model. Paper presented at the AMCIS 2017 - America's Conference on Information Systems: A Tradition of Innovation.

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.

O'Donoghue, T., & Rabin, M. (2001). Choice and procrastination. *Quarterly Journal of Economics, 116*(1), 121-160.

Oomen, I., & Leenes, R. (2008). Privacy risk perceptions and privacy protection strategies. In: Vol. 261. IFIP International Federation for Information Processing (pp. 121-138).

Pavlou, P. A., Huigang, L., & Yajiong, X. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly: Management Information Systems, 31*(1), 105-135.

Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior, 65*,
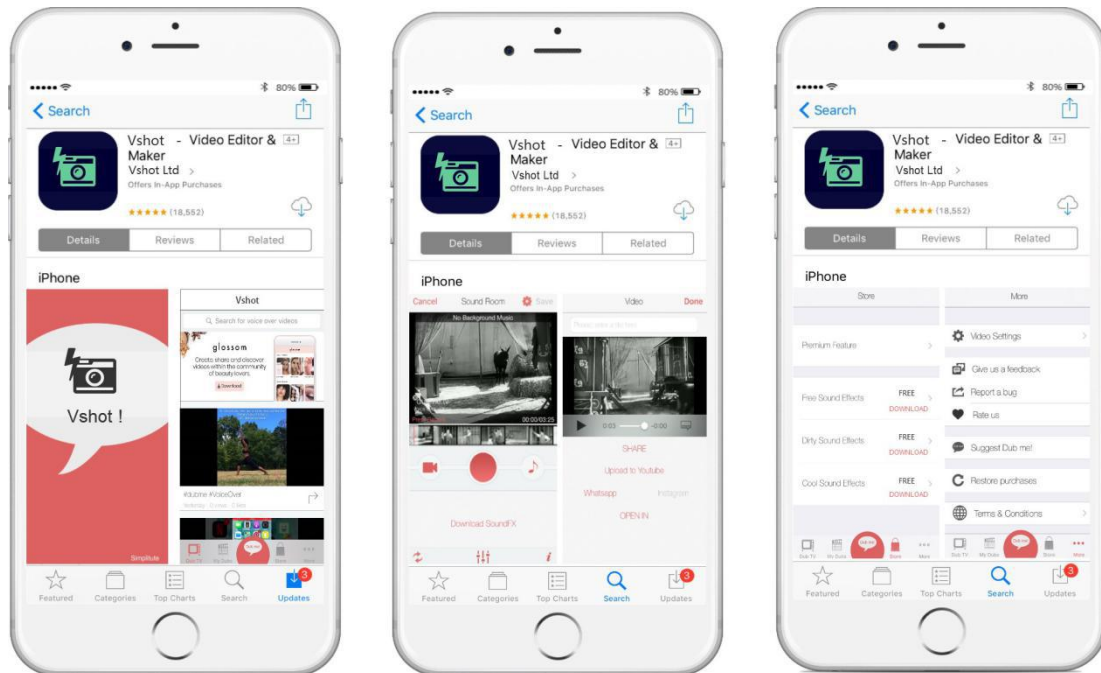
409-419.

Poikela, M., Schmidt, R., Wechsung, I., Mueller, S., (2015). FlashPolling privacy: The discrepancy of intention and action in location-based poll participation. In: Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM.International Symposium on Wearable Computers, Osaka, Japan, 813-818.

Radner, R. and Rothschild, M. (1975).On the Allocation of Effort. *Journal of Economic Theory ,10*, 358-376.

Simon, H.A., (1982). Models of Bounded Rationality. MIT Press, Cambridge, MA.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167-196.

Taddicken, M. (2014). The 'Privacy Paradox' in the Social Web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication, 19*(2), 248-273.

Tuch, A. N., Bargas-Avila, J. A., & Opwis, K. (2010). Symmetry and aesthetics in website design: It's a man's business. *Computers in Human Behavior, 26*(6),1831-1837.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bull Sci Technol Soc, 28*(1), 20-36.

Vroom, V.H., (1964). Work and Motivation. Wiley, New York.

Vilnai-Yavetz, I., & Rafaeli, A. (2006). Aesthetics and professionalism of virtual servicescapes. *Journal of Service Research, 8*(3), 245-259.

Wang, Y. J., Minor, M. S. and Wei, J. (2011). Aesthetics and the online shopping environment: Understanding consumer responses. *J. Retail. 87*(1), 46-58.

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

Xu, H., Dinev, T., Smith, J., and Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(12), 798-824.

Zhang, B., Wu, M., Kang, H., Go, E., & Sundar, S.S. (2014). Effects of security warnings and instant gratification cues on attitudes toward mobile websites. In: Toronto, O.N. (Ed.), CHI. Canada, pp. 111-114.

Zhang, D., & Adipat, B. (2005). Challenges, methodologies, and issues in the usability testing of mobile applications. *International Journal of Human-Computer Interaction, 18*(3), 293-308.

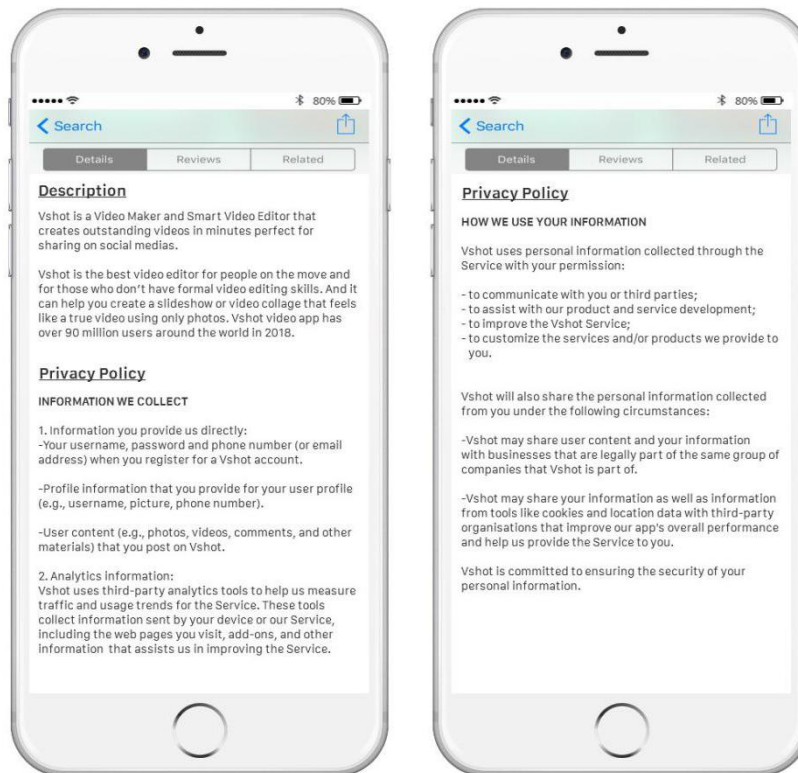**Appendix 1 Prototypes of Vshot**
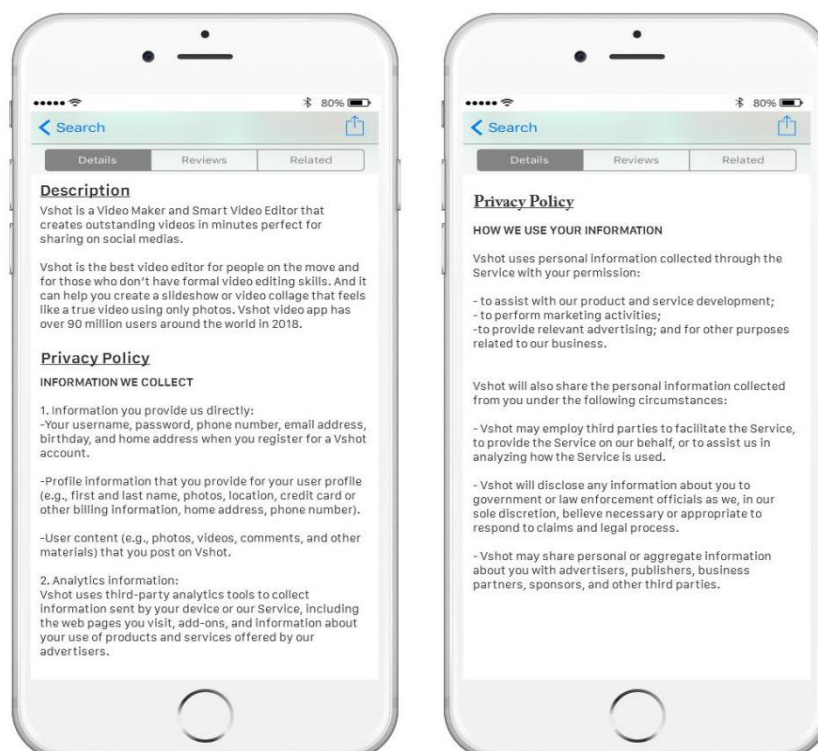

Condition 1 with high aesthetic quality

Condition 2 with low aesthetic quality

Condition 1 with low privacy threats

Screen 1 (Details):

< Search

Details | Reviews | Related

Description

Vshot is a Video Maker and Smart Video Editor that creates outstanding videos in minutes perfect for sharing on social medias.

Vshot is the best video editor for people on the move and for those who don't have formal video editing skills. And it can help you create a slideshow or video collage that feels like a true video using only photos. Vshot video app has over 90 million users around the world in 2018.

Privacy Policy

INFORMATION WE COLLECT

1. Information you provide us directly:
-Your username, password and phone number (or email address) when you register for a Vshot account.

-Profile information that you provide for your user profile (e.g., username, picture, phone number).

-User content (e.g., photos, videos, comments, and other materials) that you post on Vshot.

2. Analytics information:
Vshot uses third-party analytics tools to help us measure traffic and usage trends for the Service. These tools collect information sent by your device or our Service, including the web pages you visit, add-ons, and other information that assists us in improving the Service.

Screen 2 (Details):

< Search

Details | Reviews | Related

Privacy Policy

HOW WE USE YOUR INFORMATION

Vshot uses personal information collected through the Service with your permission:

- to communicate with you or third parties;
- to assist with our product and service development;
- to improve the Vshot Service;
- to customize the services and/or products we provide to you.

Vshot will also share the personal information collected from you under the following circumstances:

-Vshot may share user content and your information with businesses that are legally part of the same group of companies that Vshot is part of.

-Vshot may share your information as well as information from tools like cookies and location data with third-party organisations that improve our app's overall performance and help us provide the Service to you.

Vshot is committed to ensuring the security of your personal information.

Condition 2 with high privacy threats

Screen 1 (Details):

< Search

Details | Reviews | Related

Description

Vshot is a Video Maker and Smart Video Editor that creates outstanding videos in minutes perfect for sharing on social medias.

Vshot is the best video editor for people on the move and for those who don't have formal video editing skills. And it can help you create a slideshow or video collage that feels like a true video using only photos. Vshot video app has over 90 million users around the world in 2018.

Privacy Policy

INFORMATION WE COLLECT

1. Information you provide us directly:
-Your username, password, phone number, email address, birthday, and home address when you register for a Vshot account.

-Profile information that you provide for your user profile (e.g., first and last name, photos, location, credit card or other billing information, home address, phone number).

-User content (e.g., photos, videos, comments, and other materials) that you post on Vshot.

2. Analytics information:
Vshot uses third-party analytics tools to collect information sent by your device or our Service, including the web pages you visit, add-ons, and information about your use of products and services offered by our advertisers.

Screen 2 (Details):

< Search

Details | Reviews | Related

Privacy Policy

HOW WE USE YOUR INFORMATION

Vshot uses personal information collected through the Service with your permission:

- to assist with our product and service development;
- to perform marketing activities;
-to provide relevant advertising; and for other purposes related to our business.

Vshot will also share the personal information collected from you under the following circumstances:

- Vshot may employ third parties to facilitate the Service, to provide the Service on our behalf, or to assist us in analyzing how the Service is used.

- Vshot will disclose any information about you to government or law enforcement officials as we, in our sole discretion, believe necessary or appropriate to respond to claims and legal process.

- Vshot may share personal or aggregate information about you with advertisers, publishers, business partners, sponsors, and other third parties.

Appendix 2 Online Questionnaire

Q1 **Overall impression of Vshot**

	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree
1. I think Vshot is an interesting app.	○	○	○	○	○
2. I think Vshot is an attractive app.	○	○	○	○	○
3. I would like to learn more about Vshot.	○	○	○	○	○

Q2A **Willingness to download and use Vshot**

	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree
1. I would be interested in trying Vshot.	○	○	○	○	○
2. I would be willing to download Vshot on my mobile phone.	○	○	○	○	○
3. If I want to edit a video on my mobile phone, I would be inclined to try Vshot.	○	○	○	○	○
4. I would consider Vshot as a preferred app to download in the video maker category.	○	○	○	○	○

Q3 **Quality of Vshot**

	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree
1. I think Vshot offers great advantages for people who want to edit videos.	○	○	○	○	○
2. I think using Vshot will be a good experience.	○	○	○	○	○
3. I think Vshot is a well-made app.	○	○	○	○	○
4. I think Vshot is user-friendly.	○	○	○	○	○
5. I think Vshot will help me create excellent videos.	○	○	○	○	○

Q4 **Quality of Vshot**

	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree
1. I think the appearance of Vshot is attractive.	○	○	○	○	○
2. I think Vshot looks as if it is well-designed.	○	○	○	○	○
3. I think Vshot has a beautiful interface.	○	○	○	○	○

Q5 **Expected popularity of Vshot(according to rating and comments)**

	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree
1. I think Vshot must be a well-liked app.	○	○	○	○	○
2. I think Vshot is popular among users.	○	○	○	○	○
3. I think Vshot must be downloaded by many people.	○	○	○	○	○
4. I think Vshot has a high rating.	○	○	○	○	○

Q6 **Privacy aspects of Vshot**

	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree
1.I think downloading and using Vshot may threaten my personal privacy.	○	○	○	○	○
2.I would be concerned about the way Vshot handles my personal information.	○	○	○	○	○
3.It would be risky to disclose my personal information to Vshot.	○	○	○	○	○
4.I would be concerned that	○	○	○	○	○

	Vshot may misuse my personal information.				
5. I believe Vshot handles my personal information with care.	○	○	○	○	○

Q7 **Privacy aspects of Vshot**

	Disagree (25)	Somewhat disagree (26)	Neither agree nor disagree (27)	Somewhat agree (28)	Agree (29)
1. I think Vshot would collect too much information about me. (1)	○	○	○	○	○
2. I don't think Vshot will only use my personal information to improve its services. (2)	○	○	○	○	○
3. I think Vshot will share my information with other companies. (3)	○	○	○	○	○

Q8 You now have answered all the questions about the Vshot app. The following screens contain background questions, which will be used to further interpret the findings.

Q9A **Knowledge about mobile apps and privacy**

	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree
1. I know a lot about mobile phones and privacy.	○	○	○	○	○
2. I am aware of the privacy risks of mobile apps.	○	○	○	○	○
3. I know how mobile apps may invade the privacy of users.	○	○	○	○	○

Q9B **Importance of privacy**

	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree
1. I am sensitive to privacy-related issues.	○	○	○	○	○
2. I think it is important to protect my privacy.	○	○	○	○	○
3. I am really concerned about potential privacy threats.	○	○	○	○	○
4. It always bothers me when I am not aware or knowledgeable about how my personal	○	○	○	○	○

> information will be used by mobile app providers.

Q10A Please choose your gender:

○ Male (1)

○ Female (2)

Q10B Please fill in your age:

Q10C What is your nationality?

○ Chinese (1)

○ Dutch (2)

○ Other nationality: (3) _____

Q10D Please choose your currently education level:

○ High school

○ Bachelor

○ Master

○ PHD

Appendix 3 Chi-square tests

Gender*Aesthetic Quality(AQ)

	AQ+	AQ-
Male	40	42
Female	66	58

X^2=.453 Sig.(2-sided)=.571

Gender*Privacy Threats(PT)

	PT+	PT-
Male	45	37
Female	63	61

X^2=.402 Sig.(2-sided)=.572

Gender*Nationality

	Asian	Western
Male	36	46
Female	78	46

X^2=7.01   Sig.(2-sided)=.01*

Educational Level * Aesthetic Quality(AQ)

	AQ+	AQ-
Bachelor	60	44
Master	41	51
PhD	7	3

X^2=4.52   Sig.(2-sided)=.10

Education Level *Privacy Threats(PT)

	PT+	PT-
Bachelor	54	50
Master	48	44
PhD	5	5

X^2=.032   Sig.(2-sided)=.98

Educational Level * Nationality

	Asian	Western
Bachelor	61	43
Master	47	45
PhD	7	3

X^2=6.45   Sig.(2-sided)=.06

ANOVA

	Aesthetic Quality	Privacy Threats	Nationality
Age	.557	.645	.321

*p < .05.**p < .01.***p < .001

Appendix 4 Scale Construction

The convergent validity of the measurement model.

Items	1	2	3	4
Perceived Benefits (PB)				
PB1: I think Vshot looks as if it is well-designed.	0.85			
PB2: I think Vshot has a beautiful interface.	0.84			
PB3: I think Vshot is a well-made app.	0.83			
PB4: I think the appearance of Vshot is attractive.	0.83			
PB5: I think using Vshot will be a good experience.	0.81			
PB6: I think Vshot will help me create excellent videos.	0.80			
PB7: I think Vshot is user-friendly.	0.79			
PB8: I think Vshot offers great advantages for people who want to edit videos.	0.78			
Perceived Privacy Risks (PPR)				
PPR1:It would be risky to disclose my personal information to Vshot.		0.90		
PPR2: I would be concerned that Vshot may misuse my personal information.		0.86		
PPR3: I think Vshot would collect too much information about me.		0.84		
PPR4: I think downloading and using Vshot may threaten my personal privacy.		0.83		
PPR5: I would be concerned about the way Vshot handles my personal information.		0.82		
PPR6: I think Vshot will share my information with other companies.		0.78		
PPR7: I don't think Vshot will only use my personal information to improve its services.		0.75		
PPR8: I don't believe Vshot handles my personal information with care.		0.42		
Perceived Popularity				
POP1: I think Vshot must be downloaded by many people.			0.79	
POP2: I think Vshot has a high rating.			0.73	
POP3: I think Vshot is popular among users.			0.65	
POP4:1. I think Vshot must be a well-liked app.			0.47	
Download Intention				
DI1: I would consider Vshot as a preferred app to download in the video maker category.				0.85
DI2: I would be interested in trying Vshot.				0.85
DI3: I would like to learn more about Vshot.				0.83
DI4: I would be willing to download Vshot on my mobile phone.				0.80
DI5: I think Vshot is an interesting app.				
DI6: I think Vshot is an attractive app.				0.79
IDI7: If I want to edit a video on my mobile phone, I would be inclined				0.79
to try Vshot.				0.78
Cronbach's Alpha	0.92	0.91	0.94	0.91

Appendix 5

Moderation analysis of the aesthetics-related variables' effect on the relationship Privacy Threats and Download Intention

Variables	Beta	t-value	Significance
Privacy Threats (PT)	.90	2.2	p<.05
Perceived Benefits (PB)	.78	4.2	p<.001
Perceived Popularity (POP)	.55	.31	p=.76
Interaction PT*PB	-.34	-.19	p=.85
Interaction PT* POP	.05	.31	P=.76

*p < .05.**p < .01.***p < .001

Moderation analysis of the aesthetics-related variables' effect on the relationship Privacy Threats and Perceived Privacy Risks

Variables	Beta	t-value	Significance
Privacy Threats (PT)	-.23	-.16	p=.10
Perceived Benefits (PB)	-.54	-1.5	p=.14
Perceived Popularity (POP)	.68	1.9	p=.05
Interaction PT*PB	.34	1.5	p=.12
Interaction PT* POP	-.31	-1.4	P=.15

*p < .05.**p < .01.***p < .001

Moderation analysis of the aesthetics-related variables' effect on the relationship Perceived Privacy Risks and Download Intention

Variables	Beta	t-value	Significance
Perceived Privacy Risks (PPR)	-.61	-.07	p=.07
Perceived Benefits (PB)	.76	.74	p<.001
Perceived Popularity (POP)	.14	.13	p=.19
Interaction PPR*PB	.04	.05	p=.45
Interaction PPR* POP	-.03	-.03	P=.61

*p < .05.**p < .01.***p < .001

Appendix 6

Moderation analysis of the privacy background knowledge and privacy awareness effect on the relationship Privacy Threats and Download Intention

Variables	Beta	t-value	Significance
Privacy Threats (PT)	.30	.55	p=.58
Privacy knowledge (PBK)	.18	.76	p=.45
Privacy awareness (PA)	.63	2.5	p<.05
Interaction PT*PBK	-.03	-.27	p=.79
Interaction PT* PA	-.17	-1.08	P=.28

*p < .05.**p < .01.***p < .001

Moderation analysis of the privacy background knowledge and privacy awareness effect on the relationship Privacy Threats and Perceived Privacy Risks

Variables	Beta	t-value	Significance
Privacy Threats (PT)	-.20	-1.6	p=.10
Privacy knowledge (PBK)	.56	2.2	p<.05
Privacy awareness (PA)	-.12	-.43	p=.66
Interaction PT*PBK	-.12	-.78	p=.43
Interaction PT* PA	.27	1.5	p=.13

*p < .05.**p < .01.***p < .001

Moderation analysis of the privacy background knowledge and privacy awareness effect on the relationship Perceived Privacy Risks and Download intention

Variables	Beta	t-value	Significance
Privacy Threats (PT)	-.07	-1.1	p=.27
Privacy knowledge (PBK)	.01	.17	p=.86
Privacy awareness (PA)	.40	4.14	p<.001
Interaction PT*PBK	.11	1.54	p=.12
Interaction PT* PA	-.06	-.70	p=.50

*p < .05.**p < .01.***p < .001