Lost in Permissions: Accept or Deny?

Exploring the Effects of Type of Permission, Type of Review, and Type of App on People`s Risk Perceptions, Trust, Privacy Concerns, and Behavioural Intentions

Svenja Beckmann
S1629972

UNIVERSITEIT TWENTE.

Lost in Permissions: Accept or Deny?

Exploring the Effects of Type of Permission, Type of Review, and Type of App on People`s Risk Perceptions, Trust, Privacy Concerns, and Behavioural Intentions

Master Thesis

Svenja Beckmann (s1629972)

Graduation Committee

Dr. A. Beldad

Mr. M.H. Tempelman

University of Twente

Faculty Behavioural, Management and Social Sciences (BMS)

Program Master Communication Studies

Specialization Marketing Communication

Graduation Date 21 November, 2016, Enschede

Abstract

Mobile marketing has become a major issue for almost every kind of business, but notably in the context of mobile applications (apps). Especially privacy and security issues have received growing attention as consumers are becoming aware of apps collecting their personal information. This often results in a lack of trust, higher privacy concerns, increased risk perception, and lower download intentions among users. By dividing apps in hedonic (pleasure-oriented) and in utilitarian (goal-oriented) apps, this study explored the underlying factors that impact consumers' decisions to download mobile applications. Those insights might be interesting for marketers and app developers as they could incorporate those aspects into their future marketing strategies in order to increase download numbers.

This study explored the influence of type of permission, type of review, and type of app on consumers` risk perception (general, technical, and security risk), trust, privacy concerns, and behavioural intentions (download intention, WOM intention). Also, general privacy attitude was included as a covariate since it was expected that people who are generally concerned about their privacy might react more sensitive to the manipulation of type of permissions requested, the type of review they read, or the type of app in question.

Therefore, a 2 (type of app: hedonic vs. utilitarian) by 2 (type of review: positive vs. negative) by 2 (type of permission: high sensitive vs. low sensitive) experimental design was conducted with 262 German app users. Respondents were randomly assigned to one of the eight scenarios used in the study. Most participants were in the age group between 20 and 29 years and had a Bachelor`s degree or something comparable. This study revealed that especially high sensitive permissions requested by apps increase users` privacy concerns and their security risk perception, which negatively influenced their intention to download the app and recommend it to others. Correspondingly, the German participants in this study were found to be generally highly concerned about possible privacy violations and risks involved in the download of mobile applications. Furthermore, the results showed quite similar effects for type of app and type of review, by affecting almost all seven dependent variables, despite users´ privacy concerns and security risk perception. It was also shown that the influence of type of review is not dependent on the type of app. Especially users` trust in the app appeared to be significantly lower in case of a negative review as well as in case of a hedonic app. Finally, an interaction effect of type of review and type of permission on users` trust was found.

Based on the findings of this study, marketers and app providers would be well advised to not dismiss users' privacy concerns and risk perceptions. In order to counteract the adverse effects on users` intentions, app providers and marketers should emphasise their safety precautions for the protection of users' personal information. This may help to ease off users' concerns about the handling of their personal information and positively affect their attitudes and related behaviours by increasing trust. Moreover, reasons to explain why certain data is collected should be given since this is known to reduce users´ uncertainties. Also, users should be encouraged to educate themselves about privacy settings and the technical aspects of permissions. A broader knowledge in this area could increase trust and download numbers, as ignorance might lead to a refusal to grant permissions of any kind.

Keywords: *mobile apps, permissions, reviews, privacy, trust, risk perception, download intention, WOM intention*

Acknowledgements

There are several people that I would like to sincerely thank for supporting me during the whole course of my Master and during the process of writing my Master`s thesis.

First I would like to thank Dr. Ardion Beldad for being my first supervisor and for supporting me with his excessive knowledge gained from his experience as a researcher. Second, I would like to thank Mr Mark Tempelman, my second supervisor for his useful feedback and interesting aspects during the meetings. Especially the manner of open communication and possibility to discuss certain aspects with the supervisors was very pleasant to me as a German student, since the manner of communication between teachers, supervisors or managers and students can be quite stiff and hierarchical in Germany. Also, I would like to thank Lena Lindemeier for the last years we spent together during the Bachelor at Saxion University and the Master at the University of Twente. Lena, you rock!
Finally, and most importantly, I would like to thank my friends and family for supporting me in the last years, you always believe in me. I appreciate that.

Thank you all!!

Table of Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

APP	Mobile applications
HP	Hedonic app
HPHSP	Hedonic app + high sensitive permission
HPLSP	Hedonic app + low sensitive permission
HSP	High sensitive permission
LSP	Low sensitive permission
MANCOVA	Multivariate analysis of covariance
MANOVA	Multivariate analysis of variance
NR	Negative review
NRUP	Negative review + utilitarian app
NRHP	Negative review + hedonic app
NRHSP	Negative review + high sensitive permission
NRLSP	Negative review + low sensitive permission
PR	Positive review
PRUP	Positive review + utilitarian app
PRHP	Positive review + hedonic app
PRHSP	Positive review + high sensitive permission
PRLSP	Positive review + low sensitive permission
UP	Utilitarian app
UPHSP	Utilitarian app + high sensitive permission
UPLSP	Utilitarian app + low sensitive permission
WOM	Word of mouth
e-WOM	Electronic word of mouth

1. Introduction

Nowadays, smartphones have become an essential gadget for most people. King (2012) states that mobile phones are much more than pure technical devices and describes them as “private and personal devices” (p.3) as people incorporate them into their daily activities ranging from business to shopping, communication, or personal life (King, 2012; Shklovski, Mainwaring, Skúladóttir, & Borgthorsson, 2014; Wu, Huang, Yen, & Popova, 2012). Correspondingly, Lane (2012) states that “smartphones are highly personalized devices which potentially contain a lot of sensitive information about a user” (p. 67).

Depending on the usage purpose, consumers can download mobile applications (apps) to their smartphones from digital marketplaces (Liu, Au, & Choi, 2012), called app stores. Since the launch of mobile applications in 2008, more than 450,000 mobile applications were available for the Android market in 2012, with around 10 billion downloads. These figures are surpassed by Apple`s app store offering more than 650,000 mobile applications with more than 30 billion downloads since 2008 (Lin, Amini, Hong, Sadeh, Lindqvist, & Zhang, 2012).

Based on their consumption values, mobile applications can be categorized into two main groups. The first type are utilitarian apps that provide functional and practical values to the users. Their consumption is known to be “more cognitively driven” (Dhar & Wertenbroch, 2002, p. 61), or “performance-oriented” (Xiang, Jing, Lee, & Choi, 2015, p. 122). A calendar app, for example, can help users to better organise their daily tasks. The second type are hedonic apps that provide values related to entertainment, by evoking feelings of pleasure, fun, or curiosity such as gaming or music apps. Thus, hedonic apps provide “self-fulfilling values, rather than instrumental values” (Xiang et al., 2015, p.124). Research has shown that especially the functional value of an app has a positive influence on consumers’ intentions. However, it depends on each individual consumer or usage purpose to determine which features or functions are important and eventually motivate to download apps. Corresponding to this, Bellman, Potter, Treleaven-Hassard, Robinson, and Faran (2011) found that if consumers perceive apps as not personally relevant they are unlikely to download the app (p. 192).

In order to better personalise their marketing activities, apps collect information about consumers (Andrade, Kaltcheva, & Weitz, 2002; Hoffman, Novak, & Peralta, 1999). Prior to download, consumers have to grant permissions requested by the app. This implies that users grant access to data (stored) on their mobile device such as the current location, phone ID, photos, contact lists, or GPS information. Thus, consumers must be willing to disclose some personal information (Palvia, 2009; Wang, Yu, & Chiang, 2015; Yang & Wang, 2008). However, many apps requests access to users` resources that are not necessarily needed for the functioning of the app (Harris, Brookshire, & Chin, 2016; Iacob, Veerappa, & Harrison, 2013; Lane, 2012). Nevertheless, existing research demonstrates that consumers often do not fully understand permission requests or that they simply rely on the providers for their security and privacy (Harris, Chin, & Brookshire, 2015; Lane, 2012). It was also shown that the type of app gives no indication about possible privacy threats involved in the download of the type in question (Wang, Liao, & Yang, 2013; Barrera, Kayacik, van Oorschot, & Somayaji, 2010).

However, not all information is gained with the users´ full awareness and permission (Harris et al., 2016; Lee, Lim, Kim, Zo, & Ciganek, 2015; Lin et al., 2012). Harris et al. (2015) found that 87% of the participants were concerned about apps collecting or/and accessing their personal information (p.4). Specifically in the online environment, the most dominant risks are personal privacy violations, the loss of control of the (amount of) data collected, the access of personal information by third parties as well as how the collected information may be used for secondary purposes (Culnan & Armstrong, 1999; Culnan, 1993; Wang, Lee, & Wang 1998; Wu et al., 2012). Nevertheless, although consumers are concerned about their personal information being collected or accessed, this does not deter them from

downloading mobile apps, even if they perceive an app as potentially risky. This is known as the privacy paradox, where the intention and actual behaviour diverge. By drawing on the privacy calculus theory, Wu et al. (2012) explain that consumers tend to trade off risks against benefits when uncertainty about the outcomes is high. Thus, the more valuable the outcome is perceived by consumers, the more likely they are to disclose personal information (p. 891). Corresponding to this, research on behavioural decision making by Ahmad (2012) showed that the type of choices consumers make are often dominated by their emotions, rather than being cognitively driven. Thus, emotions such as the feeling of pleasure from using the app can outweigh potential risks.

Generally, trust is a crucial aspect for any kind of business as it increases consumers´ willingness to disclose personal information, which is a prerequisite for the download of an app. (Lee et al., 2015; Li et al., 2015; Palvia, 2009; Wang et al., 2015). Bergström (2015) states that trust decreases consumers' concerns about possible threats to their privacy. Thus, consumers having trust in a certain app might be less concerned about the permissions requested by the app. Furthermore, privacy concerns were found to be diverse and vary depending on the type of application (p. 419). It is therefore important for app developers and marketers to increase consumer trust in order to achieve higher number of downloads.

However, due to the fast growth of the market, many applications fail to establish a trusted and well-known brand, which is known to reduce consumers´ uncertainty and risk perceptions (Grazioli & Jarvenpaa, 2000; Jarvenpaa & Tractinsky, 1999). Moreover, prior research showed that risk perception is the most influential factor on users` intentions, with security and privacy risk being the two predominant ones (Xiang et al., 2015, p. 122-123; Harris et al., 2015; Lane, 2012) as consumers are often uncertain about their decisions when downloading mobile apps (Hoffmann et al., 1999; Nam, Song, Lee, & Park, 2006; Rouibah, Lowry, & Hwang, 2016).

Research found that in order to reduce uncertainty, consumers tend to rely on star ratings, full text reviews and word of mouth, since those are highly trusted information sources. (Kelley, Consolvo, Cranor, Jung, Sadeh, & Whehterall, 2012; Liu et al., 2012; Okazaki, 2009). Consumer reviews can be described as non-commercial recommendations of other users that involve evaluations about "user-perceived quality based on actual usage experience and satisfaction" (Hoon, Vasa, Schneider & Grundy, 2013, p. 4). Nevertheless, consumers read reviews not only to obtain product-related information but also to evaluate potential security risks involved in the download of an app (Harris et al., 2015). The problem with this is that reviews are mostly based on performance and functional related aspects which makes them unreliable indicators of possible security and privacy risks. Hence, consumers often underestimate or even are not aware of possible privacy threats when considering to download mobile applications (Chia, Yamamoto, & Asokan, 2012; Harris et al., 2015; King, 2012).

So far, research on the factors that motivate, influence, and eventually convince or deter customers to download mobile applications is scarce. Only few studies have investigated consumers' usage and adoption behaviour of mobile apps (Harris et al., 2015; Harris et al., 2016; King, 2016; Rouibah et al., 2016; Sjörberg, Moen, & Rundmo, 2004), so this research field is still relatively unexplored. Especially research on smartphone users` expectations in relation to various risks is lacking, although it is known that they affect consumers' behavioural intentions (King, 2012).

The insights gained from this study might be interesting for researchers, marketers and app developers as mobile marketing has become a major issue for most businesses. In order to increase downloads and the revenue generated with apps, it is necessary to explore and understand the most dominant factors influencing customers in the decision making process (Kim, Kankanhalli, & Lee, 2016). The results may therefore provide guidance to marketers and app developers and could stimulate the

promotion of their apps by more closely investigating consumers' information sensitivity in the context of mobile applications.

No research has been found that combined type of app, type of review and type of permission, as those variables have only been studied separately so far. Therefore, this study will try to fill the research gap by exploring the effects on people`s trust, privacy concerns, risk perception, and their behavioural intentions. Based on the previously mentioned findings, the research question underlying this study is the following:

RQ1: *To what extent do different types of app, type of review and type of permission requested to access users` phone or tablet-related information influence people`s privacy concerns, trust, risk perceptions, and their behavioural intentions?*

In the following sections, the expected effects of the independent as well as dependent variables will be described. Furthermore, results of existing research will be discussed, followed by the method of the 2x2x2 experimental design underlying this study, which will be explained in more detail. Next, the experimental approach to test the model is provided, followed by the reported findings of the study. Finally, the results as well as practical implications and limitations of this study will be discussed.

2. Theoretical Framework

A mobile application can be defined as "application software that can be installed and run on a range of portable devices such as smartphones and tablets" (Liu et al., 2012, p. 2). However, there is a diversity of mobile applications offered on the market, which might sound beneficial from a consumer's perspective. Unfortunately, there is another side of the coin. Full control over data is a complex issue in the digital environment and especially apps are known to continuously collect information about their users.

In order to download an app, users have to grant the app access their personal information and/or data stored on the mobile device. Hence, consumers must be willing to disclose some personal information which can be defined as "information identifiable to an individual" (Culnan et al., 1999, p. 105; Palvia, 2009; Wang et al., 2015; Yang & Wang, 2008). Especially for businesses, the use of mobile applications has become an important way to collect consumer related information in order to better personalize their marketing activities. (Andrade et al., 2002; Hoffman et al., 1999). Already in 2010, IKEA offered its consumers the download of a free app in order to provide them with information about special offers, guide consumers to the nearest store, or help them to decide whether the furniture would fit in their homes. (Agius, 2014; Alnawas & Aburub, 2016; IKEA, 2016). Needless to say, the underlying motivation of IKEA is to not only to support, but rather to influence consumers' buying intentions in order to increase turnover.

Generally, consumers` concerns about their information privacy have received growing attention in recent years (Benenson & Reinfelder, 2013; Harris et al. 2015; Wang et al., 1998). Bansal, Zahedi, and Gefen (2016) define privacy as "the right to control and decide what personal information is transmitted to others" (p.3). Xu, Luo, Carroll, and Rosson (2011) define information privacy as "the ability of the individual to control the terms under which personal information is acquired and used" (p. 43). A study conducted by Harris et al. (2015) found that 87% of the participants were concerned about apps collecting or/and accessing their personal information (p.4). Nevertheless, whether app providers treat users` personal information really as private often remains questionable. Since 2011, Apple has been sued for privacy violations several times, for sharing user related information with advertisers without users' approval. Subsequently, in 2012, several apps offered in the Apple Store were found to access, collect and store user information without prior permissions and without informing users about the data collection (PCWorld, 2011; TheVerge, 2012). The aforementioned findings illustrate why especially privacy and security risks have become the most dominant obstacles that prevent consumers from downloading apps or engaging in certain online transactions (Bergström, 2015, p. 425; Hann, Hui, Lee, & Png, 2002; Nam, Song, Lee, & Park, 2006; Smith, Dinev, & Xu, 1996; Woo, 2006).

2.1. Risk Perceptions in the Digital Context

Research by Kim, Ferrin, and Rao (2008) identified the three prevailing types of risk in the online environment as financial risk, product risk, and information risk. Bauer, Reichhardt, Barnes, and Neumann (2005) argue that, in regard to mobile marketing, the predominant risk is related to data security involving "data manipulation, unauthorized data access and unwanted tracking of usage patterns" (p. 185). Consequently, the perception of risk is highly influential on the willingness to adopt certain technologies (p. 186). Smith et al. (2011) define perceived risk as "the potential loss associated with the release of personal information" (p. 1001). Featherman and Pavlou (2003) define it as "the potential loss in the pursuit of a desired outcome of using e-services" (p. 454). A more general definition is given by Sjöberg et al. (2004), who perceive risk as "the subjective assessment of the probability of a specified type of accident happening and how concerned we are with the consequences "(p.8). However, the categorization of perceived risk in several dimensions is

controversial among researchers. While some divide risks in four specific categories in regard to performance, financial risks, privacy risk, and product delivery risk (Chiu, Wang, Fang, & Huang, 2014; Cunningham, 1967; Featherman & Pavlou, 2003) others prefer to use an overall measure to investigate the perception of risk (Jacoby & Kaplan, 1972). For the study at hand, perceived risk has been divided in three separate constructs, which are general risk perception, technical risk perception (related to performance/functionality) and security risk perception. By referring to earlier work by Chiu et al. (2014), those risks can be defined as follows: 1) General risk perception is based on how dangerous people perceive the download or use of a mobile app. 2) Security risk perception is based on the infringement of personal data (e.g. access of unauthorized parties and the transfer of personal data to third parties). 3) Technical or performance risk perception is based on the functioning of the app in regards to possible errors, or as "the probability that a product purchased may result in a failure to function as expected" (p. 92).

2.2 Trust and Privacy Concerns in the Digital Context

Besides risk perception, trust has also been found to be a strong predictor of consumers` decisions in the online environment (Kim et al., 2008, p. 4). Moreover, existing research clearly indicates that trust and privacy concerns are the most important factors influencing consumer behaviour in the digital context (Harris et al., 2016; Hoffmann et al., 1999; Kelley et al., 2013; King, 2012; Nam et al., 2006; Metzger, 2004; Taylor, Davis, & Jillapalli, 2009). Lee et al. (2015) define trust as "a consumer's confidence in the quality and reliability of the services offered" (p. 6), while Dooney and Cannon (1997) define trust as the "perceived credibility (ability to keep promises) and benevolence (interest to seek joint gain) of a target of trust" (p. 6). Current research by Bergström (2015) found that trust decreases consumers` privacy concerns. Moreover, the degree to which consumers see their personal information at risk may depend on a certain type of application, since the permissions requested by apps are diverse (p. 419). More importantly, Lee et al. (2015) found trust to be an important aspect for information sensitivity (p.54), which has been found to be "an antecedent of privacy concerns and related behaviours" (p. 53). Corresponding to this, Barkhuus and Dey (2003) argue that privacy concerns are not only dependent on the type of information requested but also on the perceived usefulness of the app to the user (p. 703). The explanation for this is grounded in the theory of privacy calculus (Lee et al., 2015). Current research by Wang, Duon, and Chen (2016) demonstrated that when users are concerned about their privacy, they tend to set benefits off against costs (p.539). Moreover, perceived benefits can outweigh potential risks and thereby have a stronger impact on the consumers` intentions to disclose personal information (Keith, Thompson, Hale, Lowry, & Greer, 2013).

2.3 Behavioural Intentions in the Digital Context

Most explanations on behavioural intentions are grounded on the theory of reasoned action (TRA) and theory of planned behaviour (TRB), developed by Fishbein and Ajzen, (1975), who define an intention as "the decision to act in a particular manner" (as cited in Taylor et al., 2009, p.7). Based on this, Taylor et al. (2009) define behavioural intention as "the likelihood that a consumer will engage in desired behaviour, including making future purchases, spreading positive word-of-mouth or expressing favourable opinions" (p. 8). Drawing on earlier work by Harris et al. (2016), the present study is based on the assumption that in order to being able to use a mobile app, it has to be installed beforehand, not necessarily implying that it will be used afterwards (p. 442).

A study of Xiang et al. (2010) revealed that the most influential factor on people`s intentions is perceived risk, with security and privacy risk being the two predominant ones (p. 122). Those risks are related to financial losses but also privacy violations (p. 123). A study conducted by Lee (2009) tested the influential factors for the adoption of mobile banking technologies. The results indicated a negative influence of security and privacy risks on users' intentions (p.132). Correspondingly, Chiu et al. (2014)

found that risk perception is a strong predictor of consumers' intentions in the initial as well as in the repeated purchase intention (p.92). Furthermore, prior studies have already demonstrated that attitudes and behaviours are positively influenced by trust (Pennington, Wilcox, & Grover, p. 203; Rouibah et al., 2016). Harris et al. (2016) found that strong predictors of the actual behaviour of consumers are their intentions. Moreover, the authors found a strong negative influence of perceived risk on the intention to install an app, but a positive influence of trust on the intention to download apps. Also, perceived benefit has been found to positively impact the intention to download apps.

Another intention in the context of mobile applications is word-of-mouth (WOM) which describes the "face-to-face conversation between consumers about a product or service experience" (Sen & Lerman, 2007, p. 77). Existing research shows that especially personal recommendations provided by close relatives and friends are highly trusted and eventually impact consumers´ intentions. In the context of mobile applications, Hsu, Lin, Fu, and Hung (2015) define WOM as "the act of promoting the app to others" (p. 421). Kim, Kankanalli, and Lee (2016) define it as "the communication of positive evaluation from other users about the target app" (p. 6). Earlier work by Baber, Thurasamy, Malik, Sadiq, Islam, and Sajjad (2016) and Cheung and Thadani (2012) clearly demonstrated that WOM has a strong influence on purchase intention. Consumers tend to have higher trust in recommendations of other consumers or relatives since they expect marketing purposes behind the information provided by organisations (Camarero & San Jóse, 2011; Iacob et al., 2013; Kelley et al., 2012).

A great part of information sharing today takes places via digital channels like email, blogs, or online reviews, called electronic word-of-mouth (Carmarero et al., 2011; Filieri, 2015). Baber et al.(2016) define online WOM as "any positive or negative statements made by a former, actual, or potential customer about a product or an organization to more than one person or institution via the internet" (p. 388). Especially organizations can benefit from WOM, since it has the potential to attract new users. Racherla, Furner, and Babb (2012) state that both, online and offline WOM have a strong influence on consumers` decision making. Based on their study, the authors suggests that offline WOM has a bigger impact on the discovery as well as on the download of mobile applications in comparison to online WOM, since many consumers download apps recommended by close relatives.

However, there are different influential factors that might have an impact on users' risk perception, trust, privacy concerns, and behavioural intentions. Three of them are going to be discussed in the following.

2.4 Permissions

As already mentioned in the previous section, the download and use of an app is subject to the acceptance of certain access requirements, also called permissions. Benenson and Reinfelder (2013) describe permissions as “static warnings that describe which data an app has access to (…)“ and which actions it performs” (p. 1).

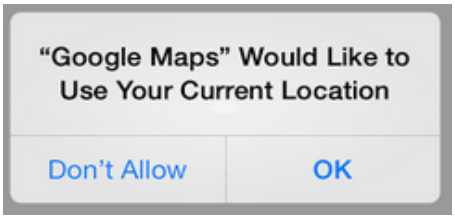


Figure 1 Permission screen iOS

However, depending on the operating system of the mobile device, permissions are treated differently by their providers. Generally, Apple reviews all apps on content, quality, and security before offering them in the app store (King, 2012, p. 2). Furthermore, Apple`s iOS makes use of a “central authority” or “centralized permission systems” (Chia et al. 2012, p. 311). This implies that users are not confronted with any technical phrases regarding the permissions requested by the app, shown in figure 1.

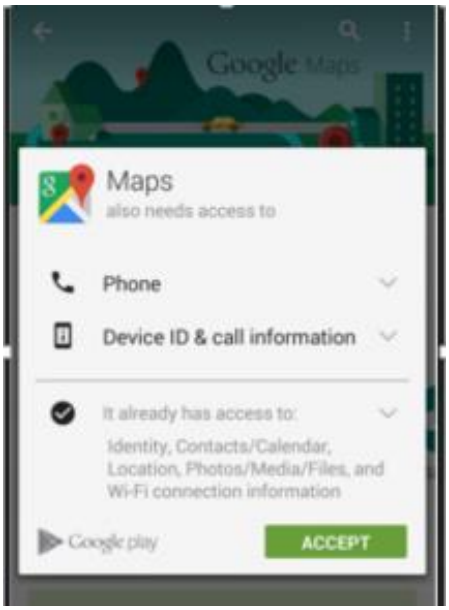


Figure 2 Permission screen Android

In comparison to that, Android makes use of the so-called “user-consent permission systems” (Chia et al., 2012, p. 311). This means that consumers are confronted with a permission screen before the actual download can be realised, listing all access requests of the app, as shown in figure 2 (Kelley et al., 2013). However, these permissions have to be accepted before the actual download takes place. Thus, the decision to grant an app access to the phone is completely left to the users. By clicking the install button, the permissions are accepted (Sarma, Gates, Potharaju, Nita-Rotaru, & Molloy, 2012, p. 15). In contrast to Apple, Android reviews its apps only on malware rather than on content, quality, or security.

The differences in the communication and handling of the permission process was found to have an influence on users’ risk perceptions. A study by Benenson and Reinfelder (2013) showed that in comparison to Android users, IOS users seem to be less concerned about privacy related issues. Moreover, it was found that 40% of Android users make use of security software, in comparison to only 6% of the iOS users (p.2). Thus, the main difference is that iOS users are not openly exposed to detailed descriptions of the permission.

2.4.1 Types of Permissions

Most apps ask for access to at least two or three resources of the users’ device such as the users` photos, current location, phone ID, or the contact list. Felt, Greenwood, and Wagner (2011) analysed 100 paid and 856 free applications regarding their permissions requests. They found that 93% of the free apps and 82% of the paid apps ask for one “dangerous” (Sarma et al., 2012, p. 14) permission at minimum. Moreover, it was found that permissions are not dependent on the type of app. Thus, the type of app gives no indication of the risks involved in the download of an app (Barrera et al., 2010; Felt et al., 2011; Wang et al., 2013).

Especially the variety of permissions makes it difficult for consumers to identify apps as being potentially risky (Harris et al., 2016; Kelley et al., 2012). Research by Sarma et al. (2012) showed that consumers` risk perception is smaller if the same permissions are requested by several or even similar apps (p. 14). Thus, consumers become "desensitized" (Harris et al., 2015, p. 1) to the permissions, which reduces their effectiveness as warning systems for consumers.
Besides the questionable access requirements, prior research by Lin et al. (2012) has identified three main problems users have to face when confronted with permission screens: (1) the technical language used in the permission list is often difficult to understand, (2) only little information is given concerning potential privacy risks, and (3) the long and frequently displayed permission screens "make users warning fatigue" (p. 507), meaning, they get used to it and pay less attention to the permissions. The authors propose that developers should use more simple terms to describe the resources being accessed and that only those that "have a greater impact on users' privacy" should be displayed (p. 507). It is further argued that informing users about the reasons for the data collection has two advantages. Firstly, it helps them "to make better trust decision" (p. 506) and secondly, it can help to reduce their concerns due to "uncertainties" that result in an increase of the user's privacy concerns due to a lack of trust (pp. 506-507).

Also, several researchers have found that most apps request permissions that are not necessarily needed for the functioning of an app (Chia et al., 2012), which Harris et al. (2016) defines as "excessive permissions" (p.3). The results indicate that consumers are generally more careful with providing their data and are less likely to download apps requesting excessive permissions. Moreover, permissions can be distinguished according to the sensitivity of information they require which can impact users' attitudes and intentions (Ackerman, Cranor & Reagle, 1999). Bansal et al. (2016) make a distinction between different types of personal information and found that people`s willingness to disclose personal information is dependent on the type of information requested. The authors define sensitive information as the type of private information that can lead to financial losses and privacy violations (p. 3). However, some permissions are perceived as more risky than others based on the perceived sensitivity of the information requested by the app. According to Gu, Xu, Xu, Zhang, and Ling (2016) permissions such as "access to the vibrator" or "keeping device screen awake" are perceived as less risky, while those requiring access to the users´ location, contact information, or photos are perceived as highly sensitive and therefore as riskier (p. 21). Correspondingly, Eling, Krasnova, Widjaja, and Buxmann (2016) found that, besides the sensitivity of the permissions requested by an app, the amount of permissions requested also affects users` privacy concerns (p. 7-8).

Based on the previous mentioned findings, it is expected that different types of permission (high sensitive and low sensitive) will influence consumers´ intentions. More precisely, it is expected that high sensitive permissions negatively influence consumers' trust and risk perceptions and thereby eventually deter consumers from downloading and/or recommending the app to others. There is a lack of research regarding the effects of permissions especially for specific types of apps. Generally, the influence of permissions on the consumers` decision making process is a relatively new research field and therefore still unexplored. Type of permission has been added as the third independent variable in this study in order to explore the effects on people`s privacy concerns, risk perception, trust, and their behavioural intentions. Therefore the following hypotheses have been formulated:

H1. *High sensitive permissions requested by an app have a negative influence on users´ a) general risk perception, b) technical risk perception, c) security risk perception, d) trust in the app, e) privacy concerns, f) intention to download the app, and the g) intention to WOM, compared to low sensitive permissions requested by an app*.

2.5 Online Reviews

In order to reduce uncertainty due to a lack of trust, experience with a product, service, or e-vendor, consumers often rely on non-commercial recommendations by others. Moreover, Liu et al. (2012) argue that online reviews are the most influential information sources for consumers in the case of high uncertainty. Research found that 60% of consumers in the online environment consider online reviews in their decision making. It was shown that consumers have higher trust in reviews than in product descriptions provided by organisations (Iacob et al., 2013, p. 1; Kelley et al., 2012).

Like most online shops today, even App stores make use of feedback features in form of consumer reviews also referred to as "online word-of mouth" or "electronic word of mouth" (Liu et al., 2012, p.4) as described earlier. This implies that customers can evaluate the app with a number of stars, mostly ranging from one to five in combination with a short statement (Pagano & Maalej, 2013).

2.5.1 Types of Reviews

In comparison to length of reviews from general online stores, reviews of apps appear to be much shorter, comparable with the length of a tweet, mostly related to a specific version of an app (Fu, Lin, Li, Faloutsos, Hong, & Sadeh, 2013, p. 1276). Previous research on app reviews by Racherla et al. (2012) showed that most apps have on average two or three reviews. Consumer reviews can be either positive, negative, or neutral towards the product (Kennedy & Inkpen, 2006).

Research by Pagano and Maalej (2013) on reviews from 1,100 most downloaded applications revealed that most feedback contains requests on features, or user experience etc**.** Also, users mostly give reasons for their evaluations (p. 133). Furthermore, results of a study by Liu, Au and Choi (2012) indicate that consumers judge the quality of an app based on sales rank and review ratings. Also, apps at the top of the ranks receive more attention and eventually gain higher download numbers (Harman, Jia & Zhang, 2012; Pagano & Maaleij, 2013; Racherla et al., 2012).

Research by Khalid, Shihab, Nagappan, and Hassan (2015) found that most unfavourable reviews involve complaints about functional errors, requests for features, or problems encountered due to app crashes (p.70). Correspondingly, Iacob et al. (2013) found that negative reviews of apps also involve information about the size of the app, its speed, as well as comments about comparable or similar apps (p. 2). Positive reviews mostly involve information about improvements of the apps due to updates and ease of use (usability). It was also shown that users have the tendency to provide a greater amount of negative feedback (especially for lower rated and cheaper apps). Already in 1980, Weinberger and Dillon found the influence of negative reviews on purchase intentions to be stronger in comparison to positive product evaluations. Research by Ahluwalia, Burnkrant, and Unnava (2000) found that consumer trust in negative information is higher in comparison to positive information, as they expect more rational and performance related aspects to be included in these reviews. This is supported by Sen and Lerman (2007), who demonstrated that consumers tend to focus mostly on negative reviews which are weighted more heavily in comparison to positive reviews in the decision making process. A study by Ba and Pavlou (2002) revealed a positive influence of consumer reviews on trust. Therefore, consumers tend to rely on the opinions and ratings of other users to reduce uncertainty (Kim et al., 2016). Research showed that a lack of consumer trust in an app or certain provider, for example due to a negative review, can result in users deleting all apps gained from this provider (Racherla et al., 2012, p. 31). Importantly, research showed that even when customers give positive feedback for a mobile application this "does not necessarily imply recommending the app to other users" (Iacob et al. 2013, p. 4). Moreover, Palka Pousttchi, and Wiedemann (2009) found that whether an app would be recommended to others is dependent on the functionality rather than on the type of app.

As mentioned earlier, consumers judge the quality and visibility of an app based on sales rank and review ratings (Harman et al., 2012; Liu & Choi, 2012). A study conducted by Harris et al. (2015) found that (besides for general information search) consumers use reviews to identify risky apps. However, community ratings and reviews generally provide information about performance and functional related aspects. This makes them unreliable indicators concerning privacy risks (Chia et al., 2012; Harris et al., 2015; Filieri, 2015).

However, research on the effects of online reviews in the context of mobile applications is scarce. The information gained from reviews is not only useful for other consumers but also for marketers and app developers, as they provide detailed insights into usage behaviours, preferences, or complaints, which can be used for product improvements or marketing purposes. It is important for marketers and app providers to explore the key determinants of trust in the mobile environment in order to increase trust by reducing consumers´ risk perceptions (Racherla et al., 2012).

Based on the aforementioned findings, the following hypotheses have been formulated:

H2. *Positive reviews of a mobile application have a positive influence on users' a) general risk perception, b) technical risk perception, c) security risk perception, d) trust in the app, e) privacy concerns, f) intention to download the app, and g) intention to WOM, compared to negative reviews of a mobile application.*

2.6 Mobile Applications

Another influential factor concerning consumers` risk perception, trust, privacy concerns, and behavioural intentions is the type of app. Mobile applications provide different values to the users, based on their functions or using purposes (Chiu et al., 2014; Hsu & Lin, 2015). Those values can be defined as "motivational constructs that serve as a standard criterion for guiding the selection or evaluation of actions or things" and vary among consumers (Chiu et al. 2014, p. 93). Based on earlier research (Kim, Park, Kim, & Lee, 2014; Xiang et al., 2015) this study divides mobile apps into two main categories: hedonic and utilitarian applications which are going to be discussed in the following.

2.6.1 Types of Mobile Applications

Hedonic apps are used to describe entertainment and experience-related apps. They are "pleasure-oriented" (Xiang et al., 2015, p.122). Examples are book, entertainment, game, lifestyle, music, photography, social networking, sports, and travel apps (p. 7). Utilitarian apps on the other hand help users to "achieve goals efficiently and conveniently" (Kim, et al., 2014, p. 7) and are "performance-oriented" (Xiang et al., 2015, p. 122). Those are related to business, education, healthcare and fitness, medical, navigation, news, productivity, utilities, and weather.

Research showed that hedonic values play a major role in consumers` decision making processes (Kim et al., 2016). A study by Belanger, Hiller, and Smith (2002) on consumers' purchase intentions found that consumers attach more importance to pleasure-related features in comparison to features for privacy and security (p. 245). Sen and Lerman (2007) argue that the reason for this is that hedonic products "satisfy emotional wants" (p. 79), as consumers tend to perceive those aspects as more important than other aspects. Also Bauer, Reichardt, Barnes, and Neumann (2005) found entertainment to be the most important driver for the intention to positive WOM. This is supported by Yang and Zhou (2011), who found recommendations to be more likely if the app or product in question is perceived as entertaining. Several researches show that apps related to entertainment, and predominantly games, are the most downloaded and recommended types of apps (Kim et al., 2011; Bauer et al., 2005; Wang et al., 2013; Wiedemann et al., 2009).

In comparison to that, judgements on utilitarian products are more "cognitively driven, instrumental, goal-oriented, and accomplish a functional or practical task" (Sen & Lerman, 2007, p. 79). A study by Chiu et al. (2014) found that utilitarian as well as hedonic values can "outweigh the perceived risks" (p. 105). However, other researchers found that, users´ intentions to positive WOM are not dependent on type of app but rather on the perceived usefulness or personal relevance of the app (Bellman et al., 2011; Chen et al., 2009; Cheng et al., 2009). The previous mentioned findings are in line with research on behavioural decision making by Ahmad (2012), which showed that the type of choices consumers make are often "driven by emotional desires rather than cognitive deliberations" (p. 72). Thus, it was shown that emotions may dominate rational deliberations.

Another study by Eling, Krasnova, Widjaja, and Buxmann (2013) found that the decision to install an app is mainly based on three factors: Firstly, users` evaluation of the perceived value of the app, secondly, users´ assessment of the costs and risks involved in the download of the app, and thirdly, users` trust in the app (provider), since trust can decrease risk perception (p. 6). However, the authors found that those aspects are "weighted against and influenced by each other" (p 6). Thus, one factor can possibly outweigh another. Nevertheless, which factor is perceived as most important is often rather subjective, but the perceived value of an app was found to be the most influential aspect on users` decision to download mobile applications.

Still, research regarding the influence of type of app on smartphone users` attitudes and related behaviours is scarce. Therefore this study will try to help to fill the research gap. Based on the previous mentioned findings an extra research question has been formulated:

RQ2: *To what extent do risk perceptions (general, technical, security risk), privacy concerns, trust, and behavioural intentions (download intention and WOM intention) differ among respondents being either exposed to) a hedonic app or b) a utilitarian app?*

2.7 General Privacy Attitude

People in general think differently about privacy-related issues. This is called privacy attitude and can be described as "dispositional privacy concerns" (Joinson, Reips, Buchanan, & Schofield, 2010, p. 13). Lai, Kuan, Hui, and Liu (2009) define an attitude as "the predisposition to respond in a particular way toward a specified class of objects" (p. 471). It is further argued that attitudes include not only rational but also emotional aspects and are therefore rather subjective. Thus, some people are more concerned than others.

Generally, attitudes are known to influence and predict behaviours as they are (in-)consistent with an individual's attitude (Ajzen, 1985; Ajzen & Fishbein, 1977). More importantly, research showed that attitudes and behaviours are positively influenced by trust (Pennington et al., 2003, p. 203) and that consumption values have a strong impact on behavioural intentions to use mobile apps (Wang, Liao, & Yang, 2013; p. 11). By referring to earlier work of Park, Campbell, and Kwak (2012) and on his own findings, Bergström (2015) argues that consumer who are generally more concerned about their privacy have a strong motivation to take actions to protect their personal information. Consequently, a strong believe in the right to privacy increases their concerns about privacy threats. This is supported by earlier work of Xu et al. (2011), which demonstrated that the general privacy attitude affects people`s risk perceptions, by triggering their need for control and decreasing their willingness to engage in actions that are perceived as being potentially risky. A study by Bansal et al. (2016) showed that extroverted people generally have higher levels of trust, but that trust is context-dependent. Moreover, people who, for example, enjoy the interaction with others were found to have a higher willingness to take risks and to trust (p. 13). Thus, the context and personality of individuals were found to be strong determinants of trust that influence the willingness to disclose information in the digital context. More importantly, by referring to the confirmatory-bias, the authors argue that people with

prior negative attitudes tend to “actively distrust and vice versa” (p. 5). This implies that people tend to interpret or search for information that is conform to their prior beliefs about a certain issue.

Based on the aforementioned findings, the covariate general privacy attitude was included in this study, since it is expected that mobile users with a high general privacy attitude may react more sensitive to the manipulation of the independent variables (type of app, type of permission, and type of review). It is expected that a higher regard for personal privacy leads to increased risk perception and privacy concerns and lower trust, download, and WOM intention. In order to explore the effects of general privacy attitude on mobile users’ risks perception, attitudes and related behaviours the following hypotheses have been formulated:

H3. *A high attitude towards privacy has a negative influence on users` a) general risk perception, b) technical risk perception, c) security risk perception, d) trust, e) privacy concerns, f) download intention, and g) WOM intention, compared to a low attitude towards privacy.*

2.8. Conceptual model

Based on the previous mentioned findings, the following research model underlying this study has been developed. It consists of three independent variables (type of permission, type of review, type of app) and seven dependent variables (general, technical, and privacy risk perception, trust, privacy concerns, download intention, and WOM intention). Also, the covariate general privacy attitude has been added to the model as it is expected that this has an impact on the seven dependent variables, previously mentioned. The arrows represent the expected relationships between the variables, based on existing research.

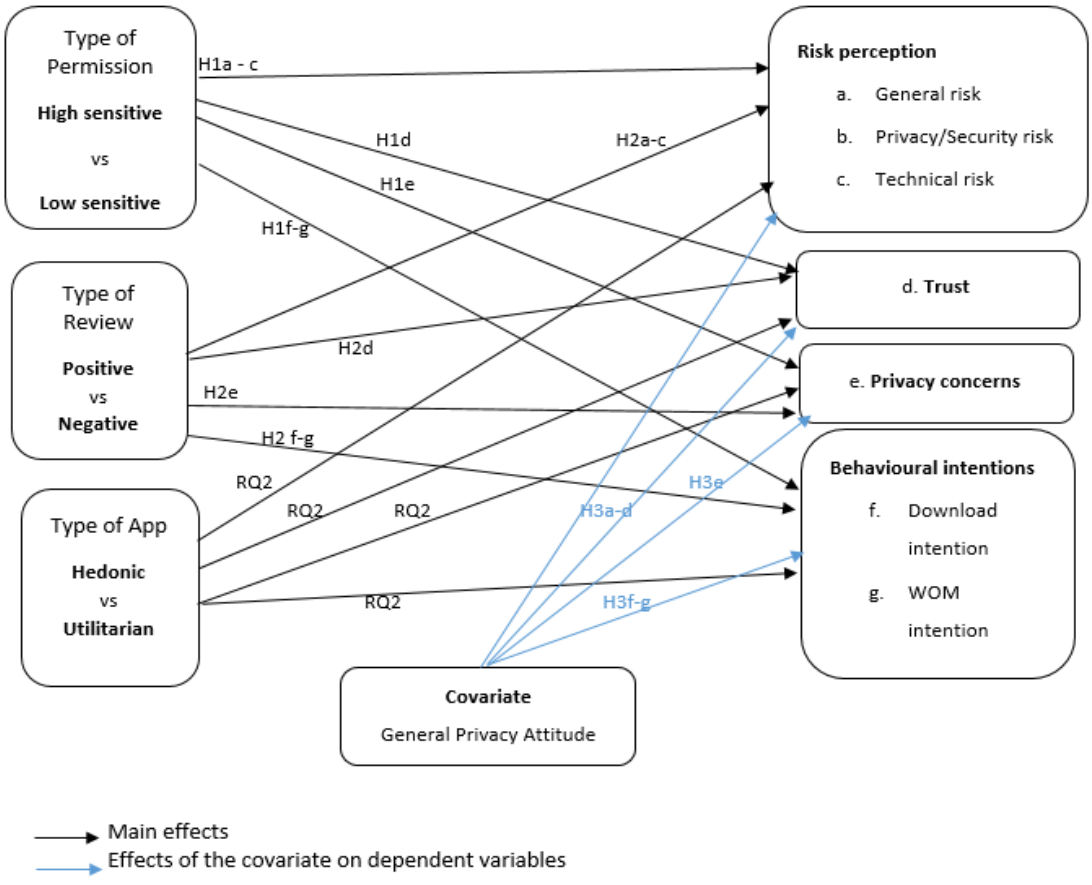


Figure 3: Conceptual Model

3. Method Section

In the following sections, the procedure and materials underlying this study are presented. Also, a description of the conceptual model and the stimuli used, as well as the procedure and measurement instruments, will be presented.

3.1 General Design

The research model underlying this study is a three-factorial (2x2x2) experimental design to test the main and possible interaction effects of type of app, type of review and type of sensitivity of information requested, on the seven dependent variables, comprised of privacy concerns, trust, general, technical, and privacy risk perception, intention to download an app, and intention to positive WOM. It is expected that the independent variables will influence people`s concerns and/or trust in the mobile application which eventually influences their behavioural intentions.

The research model is comprised out of two types of apps (hedonic vs. utilitarian), two types of reviews (positive and negative), and two types of access requirements, called permissions (high sensitive vs. low sensitive, previously shown in section 2.4. Those were manipulated in order to examine the effects on the previous mentioned variables. There is extensive research in regards to reviews/ratings on regular consumer products. Also, research on the effects of different app types and permissions have received growing attention in recent years. Nevertheless, research on the influence users` attitudinal behaviours is still scarce. Especially a combination of those variables has not been investigated before. The covariate included in the study is general privacy attitude, as it is expected that people generally having a higher tendency to worry about privacy related issues might react more sensitive to the manipulations of the independent variables.

3.2 Participants

The previous described manipulation of the three independent variables yields a total of eight combinations, that participants were randomly assigned to. All eight scenarios can be found in Appendix A. The study was solely conducted in Germany in order to avoid possible influences of different cultural backgrounds of the participants. For this study, an online-questionnaire was developed via Qualtrics and distributed in the social environment of the researcher by using email and social media (Facebook, WhatsApp). The data collection took place from 25 July 2016 until 16 August 2016. The original survey in German can be found in Appendix B.

For this study, a total set of 305 responses were collected, leading to a total set of 262 usable responses after cleaning the data set. In the study, 92 participants (35%) were male and 170 (65%) were female. The majority of participants (66%) was in the age group between 20 and 29 years, followed by people in the age group between 30 and 39 years with 21%. Furthermore, 147 out of 262 respondents (56%) used Android as operating system, and 98 respondents (37 %) used iOS. Only 13 participants (5%) used the operating system of Windows. In regards to education, it appeared that 44% of the respondents had a Bachelor's degree or something comparable, meanwhile the group of people with a Master's degree accounts for only 13%. Also, almost 30% of the participants had a high school graduation or something of equal value. On average, 33 participants were confronted with one of the eight scenarios. Table 6 shows the distribution of the respondents among the eight scenarios of the study together with the demographic information.

Table 1. Demographics and distribution of the respondents per scenario

	SCENARIO									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**Total**	**Percentage**
Gender										
Male	12	10	15	16	11	10	5	13	92	35,1
Female	28	19	24	27	19	17	24	12	170	64,9
Total	40	29	39	43	30	27	29	25	262	100
Age in years										
<20	0	0	0	2	0	0	0	0	2	0,8
20-29	28	19	24	28	18	18	22	15	172	65,6
30-39	8	5	10	10	9	6	1	6	55	21
40-49	1	3	1	1	2	1	1	1	11	4,2
50-59	2	2	3	0	1	0	3	2	13	5
60-69	0	0	1	2	0	2	2	1	8	3,1
70-79	1	0	0	0	0	0	0	0	1	2,62
Total	40	29	39	43	30	27	29	25	262	100
Education										
No degree	1	0	0	0	0	0	0	0	1	0,4
High school (medium level)	1	1	2	2	1	2	2	0	11	4,2
High school (high level)	12	11	16	7	4	6	7	10	74	7,3
Apprenticeship	2	1	2	3	5	1	3	2	19	28,2
Bachelor`s degree	17	11	17	20	15	9	14	11	114	43,5
Master`s degree	5	5	2	8	2	8	3	2	35	13,4
Doctoral degree	0	0	0	2	0	0	0	0	2	0,8
Total	48	29	37	42	27	26	29	25	262	100
Operating system										
Android	22	16	19	24	14	21	19	12	147	56,1
IOS	14	11	16	16	13	5	10	13	98	37,4
Windows	3	2	2	2	3	1	0	0	13	5,0
Others	1	0	1	1	1	0	0	0	4	1,5
Total	40	29	38	43	31	27	29	25	262	100

3.3 Stimulus Material

Before the actual main study, two preliminary studies were conducted to determine the stimulus materials used for this study.

First, the perceived sensitivity of permissions requested by the app was tested. Therefore 16 respondents were asked to rate different permissions on a 5-point Likert scale in regards to sensitivity, with (1) not sensitive to (5) very sensitive, shown in table 2. In total, 22 different permissions were presented to the participants. Those have been used based on literature (Kang, 2014; Lane, 2012) and also based on information given by Google Play store. (GooglePlay, 2016).

Table 2. Outcomes preliminary study on sensitivity

Permission request	Minimum	Maximum	Mean	SD
Photos/Media/Files: SD card content read/change/delete	**2.00**	**5.00**	**3.94**	**1.20**
In-App purchases	**1.00**	**5.00**	**2.81**	**1.24**
Identity: search/ add/delete accounts	1.00	5.00	3.88	1.17
WLAN-connection Information	2.00	4.00	3.00	0.94
Contacts: read/change personal contact list	**2.00**	**5.00**	**4.13**	**1.05**
Device ID & Call information	**2.00**	**5.00**	**4.19**	**0.88**
Location (GPS)	1.00	5.00	3.75	1.25
Camera: take pictures and videos	**2.00**	**5.00**	**4.44**	**0.86**
Information about Bluetooth Connection	**1.00**	**4.00**	**2.88**	**0.93**
SMS: read/send	2.00	5.00	4.06	0.97
Network-based location	2.00	5.00	3.38	0.86
Access to running apps	2.00	5.00	3.44	0.79
Full network access	2.00	5.00	3.88	1.05
Microphone: record audio	2.00	5.00	4.20	0.91
Device and app history	1.00	5.00	3.31	1.10
Calendar: add/ change/read information	2.00	5.00	4.13	1.15
Control over vibrate mode	**1.00**	**5.00**	**2.69**	**1.31**
Deactivate sleep mode	1.00	5.00	3.13	1.36
Change auto settings	1.00	5.00	3.44	1.12
Set alarm clock	**1.00**	**5.00**	**2.69**	**1.31**
Read Google Service configuration	**1.00**	**5.00**	**2.81**	**1.18**
Others: Create accounts and change passwords	**1.00**	**5.00**	**4.69**	**0.98**

(Note. Measured on a five-point Likert scale; the permissions used for the study are printed in bold)

Based on the outcomes of the preliminary study (table 2), for each condition (high sensitive and low sensitive) the five most dominant permissions were selected for the stimulus material (table 3). However, five out of the permissions with the highest/lowest scores were chosen for the study. A more detailed description of the permissions can be found in Appendix D.

Table 3. Permissions selected for the study

High sensitive	**Low sensitive**
1. Others: create accounts/change passwords 2. Camera: access photos, videos 3. Device ID & call information 4. Photos, media and files: read/change/delete SD card information 5. Contacts Read/change contacts	1. In-app purchases 2. Read Google service configuration 3. Information Bluetooth connection 4. Control vibrate mode 5. Set alarm clock

A second preliminary study with 16 participants was conducted to test whether respondents were able to divide 16 types of apps into their using purpose. Therefore, respondents were presented with a list with different types of apps, that they had to rate either (1) being for entertainment and pleasure or (2) to fulfil more functional values (table 4). 11 respondents were male and 6 were female. 41% of the participants were in the age group between 20 and 29 years and 18% between 40 and 49 years. The smallest age group was comprised of people between 70 and 79 years, representing only 5%. All other age groups were more equally distributed with around 11%.
The results revealed that 94% of the participants rated the music app as being used for entertainment and pleasure, meanwhile 6% rated is as being functional. 88% identified the calendar as being related to functional purposes, the remaining 12% rated it as being related to pleasure. Consequently, the results show that a calendar app (representing the utilitarian app) and a music app (representing the hedonic app) could be used for the manipulations in the main study.

Table 4. Outcomes preliminary study on app type

Type of app	Entertainment, fun, pleasure-related	Efficiency, productivity, functional	Total
Games	15	2	17
Music	16	1	17
Films/Videos/TV	17	0	17
Social networking (Facebook, Twitter)	15	2	17
Messenger (WhatsApp, Facebook)	14	3	17
E-mail	1	16	17
Calendar	2	**15**	17
Navigation	0	17	17
Dropbox	2	15	17
Fitness	7	10	17

Table 4. continued

Weather	4	13	17
News	3	14	17
Online Banking (PayPal)	2	15	17
Travel	6	11	17
Sports	11	6	17
Calculator	1	16	17

Pre-test

Before the actual main study, a pre-test with 17 participants was conducted. This was done to evaluate the comprehensibility of the scenarios, in order to collect the responses accurately. The results showed that the scenarios were interpreted as intended. The item questioning how the participants rate the review presented had to be recoded, since it was displayed in the wrong direction (from positive to negative instead from negative to positive).

3.4 Measures

In the following sections, the constructs used to measure the seven dependent variables general risk perception, technical risk perception and privacy/security risk perception, trust, privacy concerns, as well as the intention to download the app, and the intention to (positive) WOM will be presented. Furthermore, the reliabilities of the constructs are provided. All items were measured with a 5-point Likert scale ranging from (1) “strongly disagree” to (5) “strongly agree”.

General risk perception.

The construct for general risk perception is comprised of four items. Three were adapted from earlier work by Harris et al. (2016), stating “1. Downloading this app involves more risk than downloading other apps.” 2. “Downloading this app is risky”. 3. “Installing this app is harmful.” The fourth item was adapted from Stone and Gronhaug (1993) and states 4. “Downloading this app could involve important financial losses.” The construct proved to be reliable (α= 0.85).

Technical risk perception.

The items to measure technical risk perception (performance-related), were adapted and modified from Stone and Gronhaug (1993) and are formulated as 1. “As I consider downloading this app, I worry whether the app will perform as it’s supposed to.” 2. “As I consider downloading this app, I am concerned if the app is error free.” The construct was found to be reliable (α= 0.93).

Privacy risk perception.

Two items are used to measure privacy/security risk perception, which were adopted and modified from Pavlou and Chellapalla (2001). They are formulated as 1. “I am concerned that when downloading this app my personal information could be accessed by unauthorized parties.” 2. “I am concerned that my personal information could be shared by inappropriate parties.” The construct was found to be reliable (α=0.91).

Trust.

The six statements used to measure trust in the app are 1. “This app appears trustworthy to me.” 2. “I trust this app to have my best interests in mind.” 3. “I trust this app to fulfil/stick to ethical and moral standards.” 4. “I trust this app to make an effort to keep my personal information out of the hands of unauthorized individuals.” 5. “I trust this app/mobile apps not release personal information about me without my express permission.” 6.” I trust this app to fulfil its functions.” The first three items were adopted from Harris et al. (2016) and statement four and five have been adapted from earlier work by Taylor et al. (2009). The sixth item is a self-formulated item. This construct as well proved to be reliable (α=0.89).

Privacy concerns.

Three items have been used to investigate the privacy concerns of the respondents related to a mobile app. Those have been adopted and modified from existing research by Taylor et al. (2009) and Malhotra et al. (2004). The statements used are 1. “I would be concerned that information collected about me by the app could be misused.” 2. “I would be concerned that the collected data collected from the app could violate my privacy”. 3. “I would be concerned that personal information about me collected from the app could be used in a ways I did not foresee.” The construct was found to be reliable (α= 0.94).

Download intention.

The intention to download the app is measured by four items, adapted from research by Wang et al. (2013). The statements used are 1. “I will not hesitate downloading this app.” 2. “The probability that I will download this app is high.” 3. “I am most likely to download this app immediately.” 4. “I intend to use this app immediately”. The reliability analysis showed a reliable alpha value (α=0.91).

WOM intention.

The intention to positive WOM is measured by three items. Two items are adopted from existing research by Taylor et al. (2009) 1. “I would recommend this app to my friends/family.” 2. “I have positive things to say about this app”. The third statement is adapted from earlier work by Maxham et al. (2002), stating 3. “If my friends/family were looking for an app like this I would recommend this app to them.” This construct proved to be reliable (α=0.92).

Covariate.

Besides the dependent variables, the survey included a construct comprised of four items, to measure the covariate (general privacy attitude). Those four items were adapted from existing research (Xu, et al., 2011; Beldad, 2015). The statements used are 1. “For me, it is most important that my information remains private”. 2. “Compared with others, I am more concerned about potential dangers that threaten my privacy.” 3. “I think it's important that I have control over who can access my personal information.” 4. “I am convinced that my privacy should be respected and protected.” The construct was found to be reliable (α=0.84).

Type of app.

The control item for type of app was adapted and modified from existing research by Harris et al. (2016) and Kang (2014). The two statements used for the utilitarian app are 1. “This is an app for the organization of my daily tasks”, 2. “This app helps me to achieve my goals more efficiently”. The two statements used for the hedonic app are 1. “This is an app for entertainment”, 2. “This app brings me joy”. The constructs were found to be reliable (α=0.88)

The outcomes of the reliability analysis with the Cronbach Alpha values of the scales revealed a high internal consistency with values all above .80. Therefore, all constructs were included in the analysis.

3.5 Manipulation Checks

After all constructs were found to be reliable, a manipulation check was carried out in order to ensure that participants understood the manipulations as intended.

For the manipulation check, three control questions have been incorporated in the survey. By means of SPSS, t-tests were conducted to check whether the manipulations of the independent variables worked. First, after being presented to the scenario, participants were asked to rate the permissions requested by the app on a draggable bar ranging from 0 (not sensitive at all) to 100 (extremely sensitive), based on earlier research (Harris et al., 2016). For further analysis, this item has been recoded into a 5-point bipolar Likert scale ranging from 1"not sensitive at all" to 5 "very sensitive". A t-test showed a significant difference between the high sensitive condition (M=3.96 SD=1.18) and the less sensitive condition (M=3.33, SD=1.20). The results showed that the manipulation was successful ($t = 4.131$, $p < 0.001$). Nevertheless, the mean in the low condition was above the midpoint of 3, indicating that participants perceive even the low sensitive permission request as sensitive. Next, participants were asked to give their opinion on how positive or negative they perceived the previous shown reviews and ratings of the app. This was done with one item on a 5-point Likert scale ranging from 1 negative to 5 positive. It was shown that there was a significant difference between the positive reviews (M=3.99, SD=1.09) and the negative reviews (M=1.49, SD= .849). Thus, in addition a second t-test demonstrated that the manipulation was successful ($t = 20.076$, $p <0.001$).
In this study, two fictitious apps were used to avoid any influence on the results of the manipulations due to existing attitudes towards that app. Therefore, respondents were asked whether they know the app presented to them. Consequently, 12 respondents who affirmed the control question "Do you know this app" were excluded from the study. This led to a total set of 262 usable responses.

3.6 Procedure

The online questionnaire started with a short introductory welcome and a declaration of consent that participants had to accept in order to take part in the study.

Demographic questions on age, gender and highest educational achievement were asked at the beginning of the survey. Also, participants were asked about the operating system of their phone, the device used for mobile apps as well the categories of apps they mainly use.
Thereafter, before being exposed to the scenarios, four items were presented to participants, measuring their general privacy attitude. This was followed by a distraction question to shift the focus of the participants from the topic of privacy, before the actual manipulations were presented. Therefore, respondents were asked to indicate which product they recently bought online, by choosing one or several items from a short list of nine items. Subsequently, participants were randomly assigned to one of the eight scenarios.
At the beginning, participants were asked to imagine they were in the situation of searching for a certain type of app. Two types of apps were used for this study, a utilitarian app, represented as a calendar app called "My Timetable", and a hedonic app, in form of a music app called "My Beats". Both apps used were fictitious apps. Those have been chosen based on their main usage purposes, rather than on usage frequency. The aim was to have a clear distinction between the different usage purposes which was tested in the preliminary study beforehand.
First, participants were presented with a screen of a mobile device displaying reviews and ratings of other users of that app, shown in figure 2 and 3. Three different reviews have been formulated, containing comments of a) a female, n) a male and c) one anonymous given review/feedback. Previous research on reviews showed that most apps have on average 2-3 reviews (Racherla, Furner, & Babb, 2012). The reviews used in this study were either positive with an average rating of 4.5 stars (figure 4)

or an average rating of 1.5 stars in the negative condition (figure 5). The star ratings of the individual comments were ranging between 2.5 and 4 stars in the positive condition and ranging between 1 and 2.5 stars in the negative condition. This was done to keep it more realistic and to avoid people getting suspicious/sceptical due to, for example, too good or too bad ratings and comments. The content of the feedback includes mainly information about the functioning of the app, its usefulness, speed, and ease of use, but in addition a comment related to data and security has been added.

Figure 4 Positive review utilitarian app

Figure 5 Negative review utilitarian app

Next, a second screen displayed the permissions requested by the app. Those were either comprised of five low sensitive permissions (figure 6) or five high sensitive permission requests (figure 7), based on the outcomes of the preliminary, discussed in section 3.3.

Figure 6 Low sensitive permission request

Figure 7 High sensitive permission request

After being presented with the app screens, participants were asked to complete the questionnaire. The questions for the manipulation checks, control items, and the covariate were asked at the beginning, followed by the constructs for the dependent variables. The items of the survey were adapted from existing research and partly complimented with self-formulated items as described in section 3.4. At the end of the survey, participants were provided with a note expressing thanks for their participation.

4. Results

In the following sections, the main results of the study will be discussed.

In order to test for significant main and/or interaction effects, a multivariate analysis of variance (MANOVA) and a multiple analysis of covariance (MANCOVA) by means of SPSS were performed. The MANOVA analysis allows to compare multivariate population means of different groups and to explore the effects on the dependent variables due to changes in the independent variables. Also, relationships between the variables can be identified. Subsequently, a MANCOVA analysis of covariance was conducted since it allows the inclusion of a covariate and also explains the significance of the differences in the mean scores (Dooley, 2001; Dooley & Vos, 2008). Thereafter, the results of the two analyses were compared (table 7) in order to determine the influence of the covariate.

4.1 Correlation Analysis

Prior to the analysis of covariance, a correlation analysis was done to control whether the assumptions for the inclusion of the covariate are fulfilled, implying that general privacy attitude is correlated to the dependent variables (table 5).

Table 5. Correlation analysis covariate and dependent variables

Construct Dependent variable	Covariate General privacy attitude (p-value)	Pearson Correlation
General risk perception	.025*	.139
Technical risk perception	.138	.092
Security risk perception	< .001**	.360
Trust	.731	-.021
Privacy Concerns	< .001**	.369
Download intention	.068	-.113
WOM intention	.842	-.012

(Note.*. Correlation is significant at the 0.05 level (2-tailed),
**. Correlation is significant at the 0.01 level (2-tailed).)

The results of the correlation analysis indicate that three of the seven correlations are statistically significant. The correlation for general risk perception is significant at the .05 level (2-tailed) ($r(260)=.14$, $p=.025$). There is a small positive association between general privacy attitude and general risk perception, since higher levels in general privacy attitude are associated with higher levels in general risk perception. Also, a statistical significance was found for security risk perception at the .001 level (2-tailed) ($r(260)=.36$, $p< .000$). More precisely, a medium positive association was found between general privacy attitude and security risk perception implying that higher levels in privacy attitude are associated with higher levels in security risk perception. Also, a statistical significance was found for privacy concerns ($r(260)=.37$, $p<.000$), implying a medium positive association. Thus, higher levels in privacy attitude are associated with higher levels in privacy concerns.

Based on the previous mentioned findings, it is assumed that further analysis can be conducted by means of a MANOVA and a MANCOVA analysis of variance. The aim is to further explore the relation of the covariate (general privacy attitude) on the dependent variables underlying this study, as well as to identify the impact of the independent variables on this relationship. Prior to the MANOVA and the MANCOVA, the assumptions were tested in order to conduct these analyses. The results show that no serious violations were found, except the homogeneity of variance was not met for download intention ($p=.023$) and WOM intention ($p=.033$). Therefore, the results should be interpreted cautiously.

4.2 Main Effects

For a first implication about possible main effects the descriptive statistics of the independent variables were examined (table 6). With the help of the MANCOVA analysis (table 8), it was determined whether the differences in mean scores were statistically significant or not.

Table 6. Descriptive for type of app, type of review and type of permission regarding the seven dependent variables

	Mean (SD)						
	Privacy concerns	**Trust**	**General risk perception**	**Technical risk perception**	**Security risk perception**	**Download intention**	**WOM intention**
UP	3.61 (1.07)	2.76 (.79)	2.73 (.97)	2.97 (1.04)	3.55 (1.11)	1.86 (.93)	2.03 (.94)
HP	3.62 (1.00)	2.50 (.83)	2.90 (.89)	3.09 (1.17)	3.65 (1.03)	1.66 (.74)	1.92 (.87)
HSP	3.76 (1.04)	2.55 (.78)	2.89 (.92)	3.04 (1.15)	3.79 (1.07)	1.62 (.78)	1.86 (.84)
LSP	3.45 (1.00)	2.72 (.86)	2.73 (.93)	3.02 (1.06)	3.39 (1.04)	1.90 (.89)	2.10 (.97)
PR	3.54 (1.10)	2.85 (.80)	2.63 (.91)	2.37 (.78)	3.52 (1.13)	1.90 (.89)	2.24 (.95)
NR	3.73 (.94)	2.33 (.75)	3.07 (.89)	3.92 (.83)	3.71 (.98)	1.56 (.74)	1.62 (.71)

(Note. Measured on a five point Likert scale; UP = utilitarian app, HP= hedonic app, PR= positive review, NR= negative review, HSP= high sensitive permission, LSP= low sensitive permission)

The values of the Wilk`s Lambda in the multivariate test appeared to be significant for type of app ($F(7,247) = 2.11$, $p = .043$, $\eta^2 = .056$), type of review ($F(7,247) = 38.05$, $p = .00$, $p < .01$, $\eta^2 = .519$) and type of permission ($F(7,247) = 2.979$, $p = .005$, $\eta^2 = .078$) as well as for the covariate ($F(7,247) = .253$, $p < .01$, $\eta^2 = .253$). Thus, all were found to be under the significance level ($\alpha = .05$). Due to this, the Test of Between-Subjects Effects table was examined more closely to acquire more precise information about the effects of each independent variable on the dependent variables (table 7).

The results demonstrate that both analyses (with or without including the covariate) revealed similar results regarding the main effects. Differences were found regarding the interaction effect of type of app and type of permission, discussed in section 4.3.2.

Table 7. Multivariate analysis of covariance of the variables used in the study (MANCOVA and MANOVA)

	Method	Privacy concerns	Trust	General risk perception	F (p) Technical risk perception	Security risk perception	Download intention	WOM intention
Type of app	MANCOVA	.462 (.497)	**10.7 (.001)**	3.63 (.058)	**5.71 (.018)**	2.45 (.119)	**6.35 (.012)**	2.52 (.113)
	MANOVA	.007 (.933)	**10.6 (.001)**	2.82 (.094)	**4.70 (.031)**	.821 (.366)	**5.26 (.023)**	2.41 (.122)
Type of review	MANCOVA	3.00 (.084)	**33.67 (.00)**	**16.47 (.00)**	**242.18 (.00)**	3.20 (.074)	**13.02 (.00)**	**34.98 (.00)**
	MANOVA	2.82 (.094)	**33.62 (.00)**	**15.64 (.00)**	**236.18 (.00)**	2.21 (.139)	**12.32 (.001)**	**34.95 (.00)**
Type of permission	MANCOVA	**9.21 (.003)**	2.50 (.115)	1.95 (.164)	.001 (.97)	**13.38 (.00)**	**8.08 (.005)**	**4.52 (.034)**
	MANOVA	**5.94 (.015)**	2.43 (.120)	1.53 (.217)	.011 (.915)	**9.09 (.035)**	**7.16 (.008)**	**4.42 (.037)**
Type of app *type of review	MANCOVA	1.83 (.177)	.074 (.785)	.025 (.876)	1.56 (.212)	.153 (.696)	.588 (.444)	.169 (.681)
	MANOVA	1.34 (.349)	.071 (.790)	.014 (.907)	1.63 (.202)	.069 (.793)	.521 (.471)	.163 (.687)
Type of permission * type of review	MANCOVA	.006 (.940)	**5.74 (.017)**	.879 (.349)	.061 (.805)	.652 (.420)	3.44 (.065)	1.55 (.214)
	MANOVA	.012 (.914)	**5.78 (.017)**	.891 (.346)	.067 (.795)	.619 (.432)	3.44 (.065)	1.56 (.212)
Type of app * type of permission	MANCOVA	2.47 (.117)	.798 (.373)	3.34 (.069)	1.63 (.202)	3.40 (.067)	.459 (.499)	.048 (.828)
	MANOVA	**4.73 (.031)**	.900 (.344)	**4.41 (.037)**	2.39 (.123)	**5.89 (.017)**	.160 (.690)	.078 (.780)
Type of app * type of permission * type of review	MANCOVA	.629 (429)	.037 (848)	.005 (.944)	.007 (.935)	3.25 (.072)	.10 (.753)	.039 (.843)
	MANOVA	.371 (543)	.034 (855)	.000 (.983)	.001 (.973)	2.39 (.123)	.70 (.792)	.043 (.835)
General privacy attitude (covariate)	MANCOVA	**42.95 (.00)**	.170 (681)	**5.73 (.017)**	**5.44 (.020)**	**43.074 (.00)**	**5.68 (.018)**	.260 (.611)

4.2.1 Main Effects of Type of App

The following presented results are based on the outcomes of the MANOVA and the MANCOVA presented in table 7, by examining the effects with and without integrating the covariate general privacy attitude. It was shown that both analyses revealed the same main effects. The outcomes of the hypotheses testing are summarized in table 8.

General risk perception: Type of app has no main effect on general risk perception ($F(1,253)= 3.63$, $p=.058$, $\eta^2= .014$). This indicates general risk perception is not influenced by type of app.

Security risk perception: No significant main effect of type of app on security risk perception was found ($F(1,253) = .2.45$, $p=.119$, $p > .05$, $\eta^2= .010$). This suggests that the fear of a possible invasion of privacy is not dependent on the type of app.

Technical risk perception: Type of app has a main effect on technical risk perception ($F(1,253) = 5.711$, $p= .018$, $\eta^2= .022$). The score for technical risk perception turned out to be significantly higher in case of a hedonic app (M=3.09, SD=1.17) than in the case of a utilitarian app (M=2.97, SD=1.04).

Trust: Type of app has a main effect on trust ($F(1,253) = 10.7$, $p= .001$, $\eta^2= .041$). Trust turned out to be higher in case of a utilitarian app (M=2.76, SD=.79) than in the case of a hedonic app (M=2.50, SD=.83).

Privacy concerns: No significant main effect of type of app on privacy concerns was found ($F(1,253) = .462$, $p=.497$, $p > .05$, $\eta^2= .002$). This implies that privacy concerns are not influenced by type of app. Even when the covariate was included, the same effects were observed.

WOM intention : Type of app has no significant main effect on WOM intention perception ($F(1,253)= .2.52$, $p=.113$, $p > .05$, $\eta^2= .010$). Thus, the intention to recommend the app to others is not influenced by type of app.

Download intention: Type of app has a significant main effect on download intention ($F(1,253) = 6.349$, $p=.012$, $\eta^2= .024$). Download intention turned out to be higher in case of a utilitarian app (M=1.86, SD=.933) than in the case of a hedonic app (M=1.63, SD=.74).

4.2.2 Main Effects of Type of Review

General risk perception: There is a significant main effect of type of review on general risk perception ($F(1,253)= 16.47$, $p=.00$, $p< 0.001$, $\eta^2= .061$). General risk perception turned out to be higher in case of a negative review (M=3.08, SD=.90) than in the case of a positive review (M=2.63, SD=.91).

Security risk perception: Type of review has no significant main effect on security risk perception ($F(1,253)= 3.21$, $p=.074$, $p > .05$, $\eta^2= .013$). Thus, the perception of security is not influenced by type of review.

Technical risk perception: Type of review has a significant main effect on technical risk perception ($F(1,253) = 242.18$, $p=.00$, $p < .001$, $\eta^2= .489$). Technical risk perception turned out to be higher in case of a negative review (M=3.92, SD=.83) than in the case of a positive review (M=2.37, SD=.78).

Trust: Type of review has a significant main effect on trust ($F(1,253) = 33.69$, $p=.00$, $p< .001$, $\eta^2= .117$). The score for trust turned out to be higher in case of a positive review (M=2.85, SD=.80) than in the case of a negative review (M=2.33, SD=.75).

Privacy concerns: The analysis of variance was used to investigate whether privacy concerns are influenced by type of review. No significant main effect of type of review on privacy concerns was found ($F(1,253) = .462$, $p=.497$; $p > .05$, $\eta^2= .012$).

WOM intention: Type of review has a significant main effect on WOM intention ($F(1,253) = 34.98$, $p=.00$, $p< .001$, $\eta^2= .121$). The intention to positive WOM turned out to be higher in case of a positive review ($M=2.24$, $SD=.95$) than in the case of a negative review ($M=1.62$, $SD=.71$).

Download intention: Type of review has a main significant effect on download intention ($F(1,253) = 34.98$, $p=.00$, $p < .001$, $\eta^2= .049$). Download intention turned out to be higher in case of a positive review ($M=1.90$, $SD=.89$) than in the case of a negative review ($M=1.56$, $SD=.74$).

4.2.3 Main Effects of Type of Permission

General risk perception: The analysis of variance revealed that type of permission has no significant main effect on general risk perception ($F(1,253)= 1.95$, $p=.164$, $p> .05$, $\eta^2= .008$). Thus general risk perception is not influenced by type of permission.

Security risk perception: The analysis of variance revealed that type of permission has a significant main effect on security risk perception ($F(1,253) = 13.38$, $p=.00$, $p<.001$, $\eta^2= .050$). Security risk perception turned out to be higher in case of a high sensitive permission request ($M=3.79$, $SD=1.07$) than in the case of a low permission request ($M=3.39$, $SD=1.04$).

Technical risk perception: The analysis of variance revealed that type of permission has no significant main effect on technical risk perception ($F(1,253)= .001$, $p=.970$, $p > .05$, $\eta^2= .000$). This implies that there is no influence of type of permission on technical risk perception.

Trust: The analysis of variance revealed that type of permission has no significant main effect on trust ($F(1,253) = 2.495$, $p=.115$, $p > .05$, $\eta^2= .010$). Thus, trust is not influenced by type of permission.

Privacy concerns: A significant main effect of type of permission on privacy concerns was found ($F(1,253) = 9.214$, $p=.003$, $\eta^2= .035$). Privacy concerns turned out to be higher in case of a high sensitive permission request ($M= 3.76$, $SD=1.04$) in comparison to the low sensitive permission request ($M=3.45$, $SD=1.00$).

WOM intention: Type of permission has a significant effect on WOM intention ($F(1,253) = 4.52$, $p=.034$, $\eta^2= .018$). WOM intention turned out to be higher in case of a low sensitive permission request ($M=2.10$, $SD=.97$) than in the case of a high permission request ($M=1.86$, $SD=.84$).

Download intention: Type of permission has a significant main effect on download intention ($F(1,253) = 8.08$, $p=.005$, $p < .001$, $\eta^2= .031$). The intention to download turned out to be higher in case of a low sensitive permission request ($M=1.90$, $SD=.89$) than in the case of a high permission request ($M=1.62$, $SD=.78$).

4.2.4 Main Effects of General Privacy Attitude

General risk perception: The analysis of variance revealed that general privacy attitude has a significant main effect on general risk perception ($F(1,253)= 5.73$, $p=.017$, $\eta^2= .022$). Thus, general risk perception is influenced by general privacy attitude.

Security risk perception: The analysis of variance revealed that general privacy attitude has a significant main effect on security risk perception ($F(1,253) = 43.06$, $p=.00$, $p < .001$, $\eta^2= .145$). Thus, security risk perception is influenced by general privacy attitude.

Technical risk perception: The analysis of variance revealed that general privacy attitude has a significant main effect on technical risk perception ($F(1,253)=5.43$, $p=.020$, $\eta^2= .021$). This implies that there is an influence of general privacy attitude on technical risk perception.

Trust: The analysis of variance revealed that general privacy attitude has no significant main effect on trust ($F(1,253) = .169$, $p=.681$, $p > .05$, $\eta^2= .001$). Thus, trust is not influenced by general privacy attitude.

Privacy concerns: A significant main effect of type general privacy attitude on privacy concerns was found ($F(1,253) = 42.95$, $p=.001$, $\eta^2= .145$). Thus, privacy concerns are influenced by general privacy attitude.

WOM intention: General privacy attitude has no significant main effect on WOM intention ($F(1,253) = .260$, $p=.611$, $\eta^2= .001$.

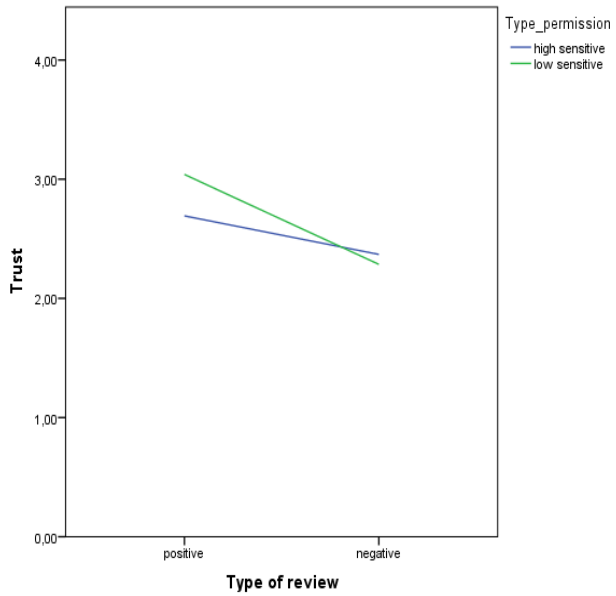
Download intention: General privacy attitude has a significant main effect on download intention ($F(1,253) = 5.67$, $p=.018$, $\eta^2= .022$). Thus, download intention is influenced by general privacy attitude.

4.3 Interaction Effects

Additionally, the analysis of variance was used to detect possible interaction effects between the three independent variables (type of app, type of permission, and type of review) and the seven dependent variables (trust, privacy concerns, risk perception, and behavioural intentions).

4.3.1 Interaction Effect of Type of Review * Type of Permission

Figure 8 Interaction effect (type of review * type of permission)



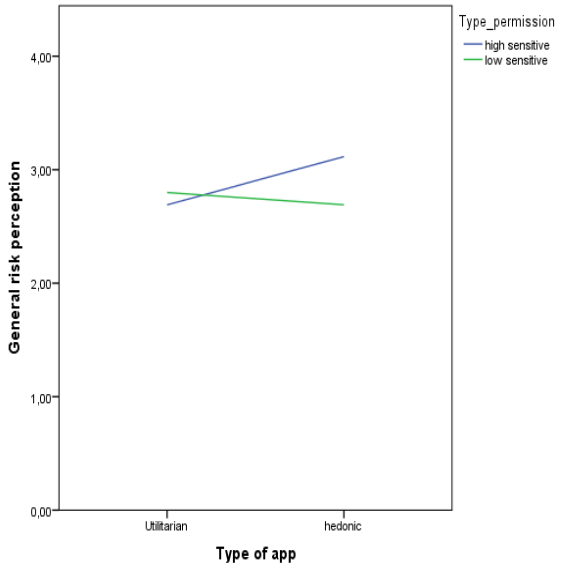
Trust: The analysis of variance revealed a significant interaction effect of type of review and type of permission on trust ($F(1,253) =5.748$, $p= .017$). Trust turned out to be higher in case of a positive review and a low sensitive permission request (M=3.06, SD=.82) than in the case of a positive review and a high permission request (M=2.70, SD=.75). In case of negative reviews, the results show that trust is stronger affected in case of a low permission request (M=2.28, SD=.72), compared to a negative review with a high permission request (M=2.36, SD=.79). This could be due to the stimulus material used in the study, since prior analysis showed that participants generally perceive permission requests as sensitive with a mean above the midpoint of three (M=3.33, SD= 1.20) in the low sensitive permission condition (section 5.2). However, it was shown that users´ trust in the app appeared to be relatively low for both permission requests (high and low). Although in both review conditions (positive and negative) trust declines, it decreases stronger if the review displayed is negative.

Furthermore, no significant interaction effects were found on privacy concerns, general risk perception, technical risk perception, security risk perception, and download intention. All values found were above the significance level with $F(1,253, p > .05)$. This means that type of review and type of permission have no combined effects (do not influence) the dependent variables previously mentioned.

4.3.2 Interaction Effect Type of App * Type of Permission

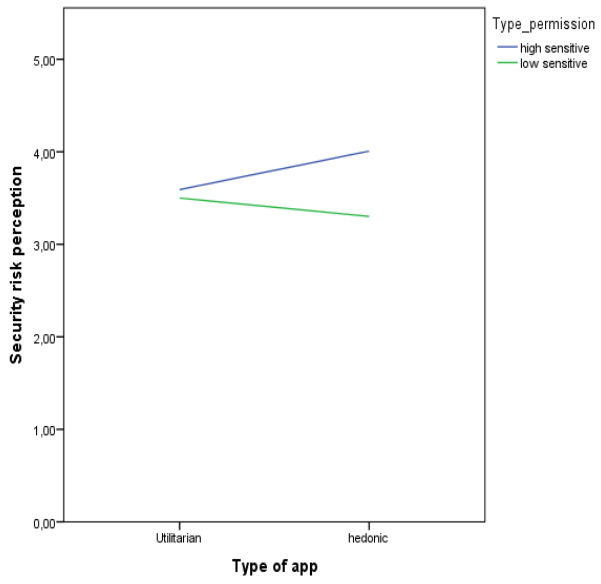
When excluding the covariate (general privacy attitude), the MANOVA showed three significant interaction effects between type of app and type of permission on general risk perception (F(1,254)= .4.40, p=.037, η^2= .017), security risk perception (F(1,254)= 5.90, p=.017, η^2=.023), and on privacy concerns (F(1,254)= 4.73, p=.031, η^2= .018). Those will be explained in the following.

Figure 9. Interaction effect (type of app * type of permission)



General risk perception: The analysis of variance revealed a significant interaction effect of type of app and type of permission on general risk perception (F(1,254) 4.40, p=.037). General risk perception turned out to be higher in case of a hedonic app in combination with a high sensitive permission request (M=3.11, SD=.86), compared to the utilitarian app in combination with the high sensitive permission request (M=2.69, SD=.93). In case of a low sensitive permission request, general risk perception turned out to be almost equal in case of the utilitarian app (M=2.79, SD=1.0), and the hedonic app (M=2.69, SD=.86).

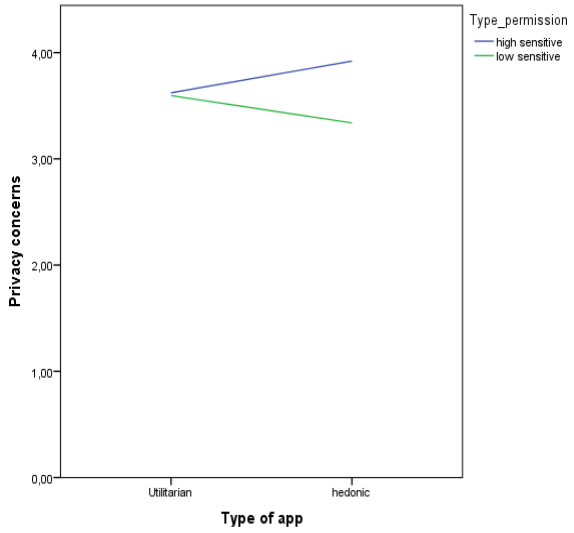
Figure 10. Interaction effect (type of app * type of permission)



Security risk perception: The analysis of variance revealed a significant interaction effect of type of app and type of permission on security risk perception (F(1,254)= 5.90, p=.017). Security risk perception turned out to be higher in case of a hedonic app and a high sensitive permission request (M=4.00, SD=.93) than in case of a utilitarian app and a high sensitive permission request (M=3.59, SD=1.15). In case of a low sensitive permission request, security risk perception decreased stronger in case of the hedonic app (M=3.33, SD=1.01), compared to the utilitarian app (M=3.50, SD=1.15).

The permissions requested by the hedonic app seem to have a stronger influence on users` risk perception (general, and security risk) than those requested by the utilitarian app. Thus, the results indicate that users are more sceptical about the hedonic app requesting high sensitive permissions, compared to the utilitarian app requesting high sensitive permissions.

Figure 11. Interaction effect (type of app * type of permission)



Privacy concerns: The analysis of variance revealed a significant interaction effect of type of app and type of permission on privacy concerns (F(1,254) =4.73, p=.031). Privacy concerns turned out to be higher in case of a hedonic app requesting high sensitive permissions (M=3.92, SD=.95), compared to the utilitarian app requesting high sensitive permissions (M=3.62, SD=1.11). In the low sensitive condition privacy concerns turned out to decrease much stronger in case of the hedonic app (M=3.33, SD=.98), compared to the utilitarian app (M=3.59, SD=1.01).

Thus, all three interaction effects indicate that (high) permissions requested by hedonic apps have a stronger influence on users´ privacy concerns, general, and security risk perception, compared to the utilitarian app. Since the focus of this study was on the main effects when including the covariate, the results of the interaction effects will not further be discussed in this paper. Nevertheless, the findings could serve as starting point for future research.

4.4 Overview Hypotheses Testing

Next, the analyses were used to determine whether the hypotheses of this study were supported or not. The outcomes are summarized in the following (table 8). The answer to the second research question **"***To what extent do risk perceptions (general, technical, and security risk), trust, privacy concerns, and behavioural intentions (download intention and WOM intention) differ among respondents being either exposed to 1) a hedonic app, or 2) a utilitarian app?"* is given in section 5.1.3.

Table 8. Outcomes hypotheses testing

	Hypotheses	Outcome
H1a	High sensitive permissions requested by an app have a negative influence on users` general risk perception compared to low sensitive permissions requested by an app	**not supported**
H1b	High sensitive permissions requested by an app have a negative influence on users` technical risk perception compared to low sensitive permissions requested by an app	**not supported**
H1c	High sensitive permissions requested by an app have a negative influence on users` security risk perception compared to low sensitive permissions requested by an app	**supported**
H1d	High sensitive permissions requested by an app have a negative influence on users` trust in the app compared to low sensitive permissions requested by an app	**not supported**
H1e	High sensitive permissions requested by an app have a negative influence on users` privacy concerns compared to low sensitive permissions requested by an app	**supported**

Table 8. continued

H1f	High sensitive permissions requested by an app have a negative influence on users` intention to download the app compared to low sensitive permissions requested by an app	**supported**
H1g	High sensitive permissions requested by an app have a negative influence on users` WOM intention compared to low sensitive permissions requested by an app	**supported**
H2a	Positive reviews of a mobile application have a positive influence on users` general risk perception compared to negative reviews of a mobile application	**supported**
H2b	Positive reviews of a mobile application have a positive influence on users` technical risk perception compared to negative reviews of a mobile application	**supported**
H2c	Positive reviews of a mobile application have a positive influence on users` security risk perception compared to negative reviews of a mobile application	**not supported**
H2d	Positive reviews of a mobile application have a positive influence on users` trust in the app compared to negative reviews of a mobile application	**supported**
H2e	Positive reviews of a mobile application have a positive influence on users` privacy concerns compared to negative reviews of a mobile application	**not supported**
H2f	Positive reviews of a mobile application have a positive influence on users` download intention compared to negative reviews of a mobile application	**supported**
H2g	Positive reviews of a mobile application have a positive influence on users` WOM intention compared to negative reviews of a mobile application	**supported**
H3a	A high attitude towards privacy has a negative influence on users` general risk perception compared to a low privacy attitude	**supported**
H3b	A high attitude towards privacy has a negative influence on users` technical risk perception compared to a low privacy attitude	**supported**
H3c	A high attitude towards privacy has a negative influence on users` security risk perception compared to a low privacy attitude	**supported**
H3d	A high attitude towards privacy has a negative influence on users` trust in the app compared to a low privacy attitude	**not supported**
H3e	A high attitude towards privacy has a negative influence on users` privacy concerns compared to a low privacy attitude	**supported**
H3f	A high attitude towards privacy has a negative influence on users` download intention compared to a low privacy attitude	**supported**
H3g	A high attitude towards privacy has a negative influence on users` WOM intention compared to a low privacy attitude	**not supported**

5. Discussion

This study to examined the effects of type of permission, type of review and type of app on people`s risk perception, trust, privacy concerns, and their behavioural intentions. This was done by means of a 2x2x2 experiment, comprised of eight scenarios participants were randomly assigned to. Existing research so far examined the three independent variables (type of app, type of review, and type of permission) only separately. No research was found that combined these three independent variables to explore their (combined) effects on consumer attitudinal constructs previously mentioned.

In the following sections the key findings derived from the study are presented. Thereafter, the theoretical and practical implications from the results will be discussed. After that, limitations and suggestions for future research will be provided, followed by the conclusion.

5.1 Key Findings

5.1.1 Main Effects of Type of Permission

The results of the study indicate that type of permission does not predict consumers' general and technical risk perception. However, the results indicate that general and technical risk perception are slightly higher in case of high sensitive permission requests, but the results were found to be not significant. A possible explanation could be that consumers are often not capable to correctly understand the meaning of the permissions requested (Felt et al., 2012; Kelley et al., 2012). Consequently, users often have the tendency to ignore those permissions and solely rely on reviews or sales rank. (Kelley et al., 2012; Liu et al., 2012). Also, consumers get used to permission requests if several apps ask for the same permission, making them ineffective as warning systems, since consumers simply do not read the permissions anymore (Sarma et al., 2012; Felt et al., 2011). Correspondingly, Harris et al. (2015) argue that consumers become "desensitized" to the permissions (p. 1). This is supported by Lane (2012), who found that "permissions have become something to quickly tap through when installing apps" (p. 69).

No influence of type of permission was found on consumers` trust in the app. For this study, it was expected that consumers would trust an app requesting high sensitive permissions less compared to an app requesting low sensitive permissions. However, trust was not affected by type of permission. Therefore, hypothesis 1d was not supported. Both (high and low) permission types showed quite similar results. More precisely, trust in the app among participants in this study generally appeared to be relatively low (M=2.50, SD=.86). Corresponding to existing literature, this could imply that consumers do not fully understand the permissions presented to them and might therefore be equally concerned for both types of permissions (Kelley et al., 2012). Existing research showed that information sensitivity is influenced by medium, personal preferences, or even the context (Ahluwalia et al., 2000; Bansal et al., 2016; Friedman et al., 2000; Xu et al., 2015). Therefore, more research is needed to exactly determine which permission requests are perceived as more dangerous than others. Finally, prior experience without any negative incidents was shown to ease off consumers concerns (Harris et al., 2015; Sarma et al., 2012).

Type of permission has been found to influence consumers` privacy concerns and their privacy risk perception, showing higher concerns in case of a high permission request. Nevertheless, research showed that consumers still download apps with high permission requests if the need or desire to have the app is strong or if apps were recommended by close relatives (Benenson & Reinfelder, 2013; Harris et al., 2015; Kelley et al., 2013; Racherla et al., 2012). A possible explanation for this could be found in the subjective norm, which can be described as "the perceived social pressure to perform or not to perform the behaviour" (Ajzen, 1991, p. 188). Moreover, Finlay, Trafimow, and Moroi (1999) state that it depends on an individual's perception "about what important others believe the individual should do" (p. 2015). In the context of this study, this could imply that, even if an individual perceives an app

as risky (e.g. due to the permissions requested by the app), the opinions of close relatives could outbalance risk perception and eventually convince to download an app after all.
However, contrary to existing research, the findings suggest that consumers do read the permissions and that they are able to recognize differences in regards to information sensitivity. Research by Kelley et al. (2012) found that consumers tend to rely on the app marketplaces for their safety by assuming that providers control apps before bringing them to the market. Hence, users tend to underestimate possible security and privacy risks (King, 2012). Also, consumers falsely expect that apps only request permissions necessary for the functioning, or even presume good reasons for the access requests (Harris et al., 2015).
Finally the results show that people`s intentions are affected by type of permission. The intention to download and positive WOM was found to be higher for an app requesting low sensitive permissions in comparison to high sensitive permissions. In other words, the less access users need to grant, the higher their intentions to engage in a certain (trans-)action. Generally, research showed that users tend to trade-off benefits against costs when considering to download apps (Lee et al., 2015; Wu et al., 2012) and that the values apps deliver can be rather subjective (Sen & Lerman, 2007). The results indicate that people are well able to distinguish between certain permission requests and, although they are willing to provide personal information to some extent, they prefer to restrict this to a minimum (Ackerman et al., 1999).

5.1.2 Main Effects of Type of Review

Type of review showed significant effects on general risk perception, technical risk perception, trust, as well as on the intention to download the app. Upon examination, it turned out that the effects were almost similar to the effects of type of app. The only difference was that no effect was found on general risk perception and the intention to WOM.

Type of review turned out to be a predictor of users´ general and the technical risk perception. Thus, based on review content, users tend to make inferences about the general risk and the risks related to the performance of an app. However, no effects were found on privacy concerns and privacy risk perception. This is corresponding to findings of Iacob et al. (2013), who found that review contents mostly involve performance-related information, for example about possible errors often due to updates, ease of use, or speed and size of the app, rather than being related to possible privacy or security risks (p. 3). Therefore, consumers might not be able to correctly gauge possible security or privacy risks when deciding to download the app.

As expected, significant effects of type of review on trust were found. It was shown that trust in the app appeared to be higher in case of a positive review than in case of a negative review. Contradictory to that, earlier research by Ahluwalia et al. (2000) found that consumers have higher trust in negative information. A possible explanation might be that if an app is personally relevant or useful to a user, he tends to focus on information and opinions that confirm these beliefs. This can be explained based on the theory of cognitive dissonance, introduced by Festinger in 1957. The theory implies that individuals consistently seek for harmony between their attitudes and beliefs. Consequently, situations in which attitudes and beliefs diverge, a feeling of discomfort arises that individuals will try to adjust. (Cialdini, 2004; Festinger, 1957; McLeod, 2014). To give an example: If a smartphone user wants to download a certain app because all his friends have it, he has a positive attitude towards the app. Being confronted with a negative review/opinion about the app would lead to disharmony between the positive attitude and the negative opinion/belief. Hence, an individual will take a certain action to restore consonance between attitudes and beliefs. This can be done in three ways. Firstly, the individual can change any of his attitudes, behaviours, or beliefs in question to, for example, avoid a certain behaviour. This would imply that, after reading the negative review, the user would adjust his positive attitude accordingly and decide not to download the app. Secondly, the user seeks new

information that can reduce the concerns. For example, the user would only look for positive reviews in order to reduce dissonance between the positive attitude and the negative belief/opinion due to the unfavourable reviews. Thirdly, the user tries to reduce the importance of the belief or attitude. In this case, the individual tries to reduce his concerns and convince himself by concluding that if all friends use this app it can`t be that bad, or friends would not recommend dangerous apps. Liang (2016) found that consumers read reviews not only prior to purchase but also after the decision has been made. Meanwhile in the pre-purchase phase, reviews are mainly used for general information seeking, while reviews are in the post-purchase phase are used to reduce cognitive dissonance, where information is selected "that support their decision to reduce cognitive dissonance" (p. 464).

Finally, significant effects were found on download intention as well as WOM intention since both were positively influenced by favourable reviews. This supports findings of existing research, which found that reviews are highly trusted and often used to reduce risk perception in situations of high uncertainty, for example when the developer is unknown, or due to a lack of experience with the app/product (Bauer et al., 2005; Liu et al., 2012; Wiedemann et al., 2009). Sen and Lerman (2007) assume that the effects of WOM can be explained by the attribution theory, developed by Heider in 1958. The theory suggests that consumers confronted with reviews tend to determine the underlying emotions that encouraged the writer of the review. Thus, readers make inferences about the underlying motivations of the writer of the review (p. 82). More precisely, readers try to assess whether the motivation was based on external motivations related to the product, or internally motivated by the individual reviewer. However, the author found that people perceive the information as more useful and credible when the review was based on external motivations, while internal motivations decrease the value of the review.

5.1.3 Main Effects of Type of App

This study examined the type of app (hedonic vs. utilitarian) will have different effects on people`s general risk perceptions, technical risk perception, security risk perception, trust, privacy concerns, and their intention to download the app, as well as the intention to recommend the app to others, also referred to as WOM intention. Due to insufficient research findings, an extra research question was formulated, namely: *To what extent do risk perceptions (general, technical, and security risk), trust, privacy concerns, and behavioural intentions (download intention and WOM intention) differ among respondents being either exposed to 1) a hedonic app or 2) a utilitarian app?* The answers to the question are provided in the following.

No effect of type of app was found on consumers' general risk perception and security risk perception, while a significant effect of type of app on technical risk perception (performance-related) was found. Technical risk perception turned out to be higher in case of a hedonic app. Meaning, consumers were more concerned about the performance of a hedonic app (M=3.09, SD=1.17) in comparison to a utilitarian app (M=2.97, SD=1.04). A possible explanation for this could be that hedonic apps, such as gaming apps or music apps, require a direct internet connection in order to use all functions of the app (e.g. to use in-app purchases, share playlists with friends). Especially if apps are used in combination with social media accounts to connect with friends, the technical performance is important (Rossi, 2010). Research by Kim et al. (2016) found that app enjoyment has a stronger influence on purchase intention than the usefulness of an app (p.12). However, no research has been found that examines those effects in more detail. Therefore, possible reasons can only be suggested and should be further explored in future research. The results of the analysis also showed that trust was significantly affected by type of app. Trust turned out to be significantly higher for the utilitarian app than for the hedonic app. The general levels of trust in the app appeared to be relatively low for both types of apps, both under the midpoint of three. Although trust and privacy concerns are known to have a strong relation (Chiu et al., 2014; Hoffmann et al., 1999; Taylor et al., 2009), no influence of type of app was found on

privacy concerns as well as on security risk perception. This demonstrates that both are no predictors of consumers` privacy and security concerns. However, existing literature showed that consumer decisions are often driven by emotions which are often perceived as more important and thereby outweigh perceived risks (Ahmad, 2012; Hsu & Lin, 2015; Kelley et al., 2016; Sen & Lerman, 2007). Contrary to existing research, the results indicate that people have higher trust in a utilitarian app compared to a hedonic app. Furthermore, the results demonstrate quite similar scores for both app types (hedonic and utilitarian) in regards to privacy concerns and security risk perception. This leads to the suggestion that they are not dependent on type of app, which is supported by earlier work of Iacob et al. (2013). Thus, consumers' concerns might therefore depend on other factors such as prior knowledge, experience, gender, context, technical expectations, or if the app is perceived as personally relevant or useful to the consumer (Ahluwalia et al., 2000; Bansal et al., 2016; Bellmann et al., 2011; Friedman et al., 2000; Xu et al., 2011).

Prior research already has shown that trust has a positive influence on consumers' intentions (Rouibah et al., 2016; Harris et al., 2016). It was expected that the intention to download and recommend the app would be higher in case of a hedonic apps since existing research showed that most downloaded and recommended apps are related to entertainment (Bauer et al., 2005; Kelley et al., 2016; Yang & Zhou, 2011). Contrary to this, the results demonstrate a higher download intention for the utilitarian app. This outcome seems difficult to generalize as it was shown that consumers only download apps that are personally relevant to them (Ahluwalia et al., 2000; Bellman et al., 2011). Also, app choice might depend on a specific situation or context, personal involvement, experience or technical expectations towards the app. Thus, those decisions might be rather subjective (Harris et al., 2015; Friedman et al., 2000; Racherla et al., 2012; Xu et al., 2011). Therefore, the results might have been influenced by the personal relevance of the app for the participants of this study, since the apps were chosen based on usage purpose, rather than on consumer involvement.

Existing research also showed that behavioural intentions are positively influenced by the functional value of a product/app, which is applicable to both types of applications (Cheng et al., 2009; Wang et al., 2013). However, WOM intention was not affected by type of app. This is contrary to existing research (Bauer et al., 2005; Yang & Zhou, 2011), that found entertainment related apps to be the most recommended apps. Nevertheless, Iacob et al. (2013) argue that even if consumers like an app this does not necessarily mean that they would recommended the app to others. This leads to the suggestion that consumers' intention is rather dependent on, for example, their satisfaction or enjoyment with the app itself, independent of the type of app in question. (Kim et al., 2016; Iacob et al., 2013; Xiang, et al., 2015). Research by Xiang et al. (2015) examined users` acceptance on different application types in relation to perceived usefulness, perceived risks, and perceived ease of use. The authors found that perceived risk had a negative influence on the intention to use utilitarian apps, while no effects were found on hedonic apps. More importantly, ease of use and perceived enjoyment were found to be the two most important factors influencing consumers. The authors suggest that app developers should therefore include emotional appealing aspects into the design of their apps.

5.1.4 Main Effects of General Privacy Attitude

Significant effects were found from the covariate general privacy attitude on users' risk perceptions, privacy concerns, and the intention to download the app. No effects were found on trust and WOM intention. General privacy attitude was measured on a 5-point Likert scale and the results showed that participants in this study had a high average score of privacy attitude (M=4.09, SD=.78). This implies that they were generally highly concerned about their privacy in the context of mobile applications. Research so far demonstrated that people who are highly concerned about their privacy tend to perceive higher risks than people with a low general privacy attitude. Consequently, this influences their behavioural intentions (Harris et al., 2016; Kim et al., 2008; Xu et al., 2011). Harris et al. (2016) found that perceived risk negatively influences the intention to install an app. This is confirmed by the

findings of this study, since the intention to download the app appeared to be relatively low among participants in this study (M=1.75, SD=.84). The correlation analysis demonstrated that general privacy attitude is correlated with general risk perception, security risk perception, as well as privacy concerns. Thus, this indicates that a high attitude towards privacy increases risk perception and privacy concerns. However, the intention to positive WOM was not influenced by general privacy attitude but was also found to be relatively low (M=1.97, SD=.90). This could be due to the fact that although people perceive their own privacy at high risk, this does not deter them from recommending an app to others, since risk perception varies among people. Furthermore, Bergström (2015) found that consumers who are highly concerned about their privacy tend to take actions to assure the safety of their personal information. Consequently, a high tendency to worry about privacy increases privacy concerns. Indeed, the findings of the study showed that participants were in general highly concerned about their privacy (M=3.61, SD=1.03). However, although privacy concerns and trust were found to have a strong relation, no effects of general privacy attitude on trust were found. Existing research showed that trust influences people`s privacy concerns (Bergström, 2015; Kelley et al., 2013; King, 2012; Metzger, 2004). Moreover, trust was found to reduce risk perception and privacy concerns. Corresponding to the high privacy concerns and the high privacy attitude, the levels of trust appeared to be relatively low among participants in this study (M=2.50, SD=.86). Thus, this indicates that the high concerns about privacy negatively influenced participants' trust in the app.

5.2 Research Implications

Based on the findings of this study, implications for theory and practice could be obtained. Those are going to be discussed in the following sections. The aim of this study was to contribute to existing research on consumer behaviour in the context of mobile applications since especially the impact of people`s risk perception and its effects on behavioural intentions are relatively unexplored.

5.2.1 Theoretical Implications

Type of Permission

First of all, the current findings suggest that type of permission is one of the key variables to predict users' privacy concerns and security risk perception by affecting users' behavioural intentions. Moreover, it was shown that high sensitive information requests increase users' privacy concerns and security risk perception, which had a negative impact on users' intentions to download and recommend the app to others. Hence, the more sensitive the information requested by an app, the lower the intention to download and recommend the app to others. This implies that users prefer to share less sensitive information. However, research so far offers no clear results about what specific types of permissions users perceive as more risky than others, since privacy concerns are often rather subjective and vary among people (Bergström, 2015; Harris et al., 2015; Friedman et al., 2000; Racherla et al., 2012; Xu et al., 2011).

Furthermore, existing research indicates that the perceptions of risks regarding privacy and security differ between Android and iOS users. Moreover, the findings suggest that iOS users are generally less concerned about possible privacy and security risks in comparison to Android users. Most participants in this study were Android users, which might have influenced the outcomes, since it was shown that participants were generally highly concerned about disclosing their personal information. However, this research field is quite unexplored and might give some new insights into the effects of the different risk communication strategies used by Google and Apple (Harris et al., 2016; Kelley et al. 2013; King, 2012).

Privacy Attitude

The results indicate that the German participants in this study were generally anxious about their privacy, which was reflected in the high general privacy attitude among the participants. Thus, they seemed to be highly concerned about the disclosure and handling of their personal information in the context of mobile applications. Consequently, they perceive their privacy at a high risk, which negatively influenced their intention to download mobile apps. Nevertheless, existing research showed that several factors can be of influence on people`s concerns about their privacy, such as prior experience, age, gender, culture, product involvement, expectations, or even context (Ahluwalia et al., 2000; Bansal et al., 2016; Bellmann et al., 2011; Bergström, 2015; Cialdini, 2004; Friedman et al., 2000; Harris et al., 2015; Hofstede et al., 2014; Racherla et al., 2012; Xu et al., 2011). This suggests that more research is necessary in this field. Also, the underlying factors that motivate or even deter consumers from trusting an app and recommending the app to others should be examined more closely, since it turned out that privacy attitude does not influence users´ WOM intention and trust in the app.

Type of Review

In this study, favourable reviews were found to positively influence users' trust in the app by decreasing their general and technical risk perception, which eventually increased their intention to download and spread WOM. This is in line with prior research findings, which demonstrated that users judge the quality or security of an app based on review ratings, sales rank, or download numbers and that online reviews are highly trusted by consumers (Harman et al., 2012; Harris et al., 2016; Iacob et al., 2013; Kelley et al., 2012; Liu et al., 2012). Existing research suggests that the effects of type of review on user behaviour vary depending on the type of app or product in question. More precisely, research indicates that unfavourable reviews have a stronger, negative effect on utilitarian products compared to hedonic products. Cheema and Papatla (2010) and Liu et al. (2012) found that online reviews have a stronger influence on hedonic products in comparison to non-hedonic products. The authors argue that this might be due to the fact that decisions for hedonic apps are often influenced by own experiences or feelings, rather than on opinions of others. However, there was no interaction effect found between type of app and type of review in this study. Nevertheless, this could be an interesting point for further investigation.

Type of App

It was shown that type of app is a predictor of users´ trust in the app, which turned out to be higher in case of a utilitarian app compared to a hedonic app. However, trust in the app appeared to be low for both types of apps used in this study. This is contradictory to existing research by Wiedeman et al. (2009), who found that apps related to emotions have the greatest influence on the willingness to try the app. In this study, only technical risk perception (related to the performance of the app) was affected by type of app. Thus, based on the type of app users make inferences about, the performance of an app which eventually influenced their download intention. Nevertheless, the intention to positive WOM was not influenced by type of app. This is in line with findings of Wiedeman et al. (2009), who demonstrated that whether an app would be recommended to others mainly depends on its functionality but not on type of app. However, research showed that users only download apps that they perceive as personally relevant (Bellman et al., 2011). Therefore, consumer involvement could be an important aspect to include for future research.

5.2.2 Practical Implications

Besides the theoretical implications, this study also provides several practical implications.

The results of the study indicate that users` risk perception has a negative influence on trust and related behaviours, which reduces the willingness to disclose personal information. Andrade et al. (2002) proposed three additional approaches to encourage consumers' willingness to self-disclose personal information, which is a prerequisite for the download of mobile applications. Those involve:

1. The development of a trustworthy reputation which is especially important for unknown or small app providers that are new on the market. Correspondingly, a study by McKnight, Choudhury, and Kacmar (2002) showed that reputation is an important aspect to build consumer trust. Especially in the early stages, consumers tend to rely on a vendor's reputation in order to reduce their uncertainty. A positive reputation can not only help to attract new customers but also retain existing users since research showed that almost 80% of apps downloaded are uninstalled after the first months (Alnawas & Aburub, 2016). However, prior research also showed that users often judge the quality and/or trustworthiness of an app by numbers of reviews, downloads, and position in ranking list (Harman et al., 2012; Kelley et al., 2012; Pagano et al., 2013; Liu et al., 2012). A study by Krasnova, Eling, Abramova, and Buxmann (2014) showed that the number of reviews has a strong influence on users` decision making process in the context of mobile apps. More precisely, the authors found that apps with about 150 reviews "signal review reliability" (p. 15). Thus, they are perceived as being trustworthy by users. Therefore, app providers should encourage mobile users not only to download their apps but also to write reviews and give ratings for them, since higher visibility in the ranking list increase user attention, eventually leading to higher download numbers. This is in line with the findings of this study which revealed that type of app and type of review significantly affect trust and users´ intentions to download the app and/or spread positive WOM.
Furthermore, prior studies showed that feedback features are an important source for developers to gain better insights into customers' needs and wants, or about failures or needed improvements of apps or new functions and features (e.g. achieve a more user-friendly design). Nevertheless, research by Liu et al. (2012) already demonstrated that there are several factors that may influence the effectiveness of reviews, such as the amount or the quality of the reviews, as well as product type or reputation of the product in question. Therefore, app providers/developers should ensure the quality of their reviews, since research showed that consumers evaluate the quality and security of an app based on reviews, download numbers, or ranking lists. However, information regarding security is mostly not involved (Harris et al., 2016).

2. Providing users with a comprehensive privacy policy was found to be a quite effective way to reduce consumers risk perception and to increase trust. This should be done by openly stating the reasons for the data being collected. Even if users do not fully read the policies provided it may increase the feeling that the protection of their privacy is assured (Andrade et al., 2002; Kelley et al., 2012; Kim & Koohikamali, 2015). Also, more detailed explanations on the permissions should be provided, since users are often not able to fully understand the technical expressions they are confronted when downloading apps. This could help users to educate themselves about privacy settings and the technical aspects of permissions, since a broader knowledge in this area could increase trust and reduce risk perceptions. Also, app providers could offer to delete users` personal information on request. The results of this study indicate that permission requests have an influence on users` privacy concerns, security risk perception, and behavioural intentions. Hence, it is important for marketers to increase trust and reduce users risk perceptions since this increases their willingness to provide personal information. Moreover, users often do not read the permissions requested by apps (Kelley et al., 2012). Therefore, the use of visual design features could support users to identify risky permissions

more easily, at first sight. Dangerous permissions or those not necessarily needed for the functioning of the app could be marked in red or printed in bold, to easily attract consumers attention without much effort. Choe, Jung, and Fischer (2013) proposed the idea to use the so-called privacy ratings. This involves that users are provided with ratings about the level of privacy protection of an app, shown in figure 12.

Figure 12 Rating for app security

This could help users to better (and more easily) detect possible risks without being overloaded with technical language or details by making permission requests more comprehensible for users. Especially older people (not belonging to the group of early adopters) may benefit from this, since research showed that age as well as prior experience influences consumers' attitudes and related behaviour regarding the adoption of technologies (Hsin Chang & Wen Chen, 2008; Kelley et al., 2009; Nam et al., 2006; Laguna & Babcock, 1997; Nowak & Phelps, 1992; Wagner et al., 2010). Correspondingly, Kelley, Breeese, Cranor, Jung, Sadeh, and Wetherall (2012) proposed to use privacy labels, similar to those commonly used in the food sector, to inform users about potentially harmful contents. However, especially in Germany, the use of labels as a form of security assurance is a common method used in e-commerce. Therefore, app stores and providers could use such labels to reduce consumers` uncertainties regarding privacy and security risk perception, as shown in figure 13 and 14.

Figure 13 App security label

Figure 14 App security label

3. Offering a reward in exchange for information transmission (e.g. offering additional features or discounts on in-app purchases) can positively impact consumes willingness to disclose personal information. Hence, the incentive offered may outweigh potential concerns and thereby encourage users' willingness to engage in a certain online transaction. This is supported by Kahnemann and Tversky (1979) who found that consumers are risk averse when losses are framed as gains. Prior research showed that consumer trade-off benefits against costs in case of uncertainty about a product or app (Lee, 2009). However, it still it remains unclear how strong the prior privacy calculation process effects consumers' intentions to engage in certain online transactions (e.g. to download or use the mobile application). Therefore, developers and marketers should highlight the advantages gained in exchange for disclosing personal information in order to shift consumers' focus from possible privacy threats on the benefits delivered by the app. For example, in the case of a calendar app (utilitarian) that requests access to users' contact lists (which can be regarded as high sensitive data), it should be highlighted that this enables users to synchronise their apps with other users like friends or family (benefit of connecting with other people). This could also positively impact the download numbers of apps since users might encourage close relatives to use the app as well. Thus, they may act as "free commercial channels" (Hsu et al., 2015, p. 426), which may help to attract new potential customers/users. Hence, this could increase download numbers and thereby the generated turnover. Nevertheless, highlighting benefits is not a guarantee to increase download intentions, since users only download apps that they perceive as personally relevant (Bellman et al., 2011).

5.3 Limitations and Future Research

This study is subject to several limitations that should be taken into account for the interpretation of the results. The generalizability of the findings is therefore limited, explained in the following.

Firstly, the data collection was restricted to only one country, Germany. Therefore the results might be subject to possible influences due to the cultural background of the respondents. Prior research by Hofstede in the late seventies demonstrated that people from the German culture seek to avoid uncertainties due to unknown situations or unforeseeable events, reflected in the country's strong need for norms, rules, or laws (Hofstede, Minkov, & Hofstede, 2014). This leads to the suggestion that this might have an impact on people`s risk perceptions and concerns about privacy in the context of mobile applications. Indeed, the findings of this study, indicate that Germans generally seem to be roughly concerned about their personal privacy (M=3.62, SD=1.04), resulting in a relatively low intention to download mobile applications. It would therefore be interesting to conduct the study in other countries, to explore whether possible cultural differences can be found.

Secondly, predominately female respondents (65%) took part in the study, which might have influenced the results. Especially in the online environment, women are known to be more concerned about privacy than men (Bergström, 2015; Graeff & Harmon, 2002). Also, men were found to have a higher willingness to use or adapt certain technologies (Akturan & Tezcan, 2012; Hsin Chang & Wen Chen, 2008; Taddicken, 2014). Hence, a more equal distribution in the eight conditions might reveal possible influences of gender.

A third limitation is the age of the participants, since most were in the age group between 20 and 39 years. Existing research states that people in the age group between 25 and 44 belong to the early adopters, growing up with certain technologies like smartphones, computers, and mobile applications (Ben-Asher et al., 2011). Thus, they tend to use and adopt technologies more naturally in comparison to older people, who might have less knowledge or experience with mobile applications. Especially in regard to the handling of personal information, existing research demonstrated that younger consumers perceive the collection of data more positive than older people. Hence, in the context of mobile applications this could imply that early adopters have a higher willingness to disclose personal information, as they are less concerned about their privacy when downloading apps (Gervey & Lin, 2000; Nam et al., 2006). Several studies have demonstrated that privacy concerns change over time and increase with age, due to, for example, physical characteristics or experiences (Hawthorn, 2000; Nowak & Phelps, 1992; Wagner et al., 2010). Laguna et al. (1997) found that computer anxiety is higher among older adults in comparison to younger people, which in turn affects their usage intentions regarding technologies (p. 324). Hence, the previously mentioned findings indicate that differences would be found in case of a more equal distribution of the age among the participants.

A fourth limitation could be the high educational background of the participants, since most had a Bachelor`s degree or something comparable. Therefore, the findings of this study cannot be generalized to the whole German population and should be extended including a more varied educational background.

5.4 Conclusion

The aim of this study was to further contribute to existing - but relatively limited - research on consumer behaviour in the context of mobile applications. Especially privacy and security issues in the digital context have received growing attention in the last years, since consumers became aware of the fact that apps constantly collect and use their personal information. However, uncertainty about the collection and handling of users´ information affects their willingness to provide personal information by increasing their privacy concerns and risk perceptions that may prevent them from downloading apps.

The study explored the effects of type of permission (high sensitive vs. low sensitive), type of review (positive vs. negative), and type of app (hedonic vs. utilitarian) on consumers` attitudes and related behaviours. The results of the study indicate that users` risk perceptions have a negative influence on their willingness to disclose personal information. Especially high sensitive permission requests were found to have a negative impact on users´ download intention, as well as on their WOM intention. Reviews, as well as type of app were found to be important determinants of users` trust in the app, which eventually affects their behavioural intentions. Especially favourable reviews were found to positively affect consumers` attitudes, related behaviours and vice versa. More importantly, it was shown that the influence of type of review is not dependent on the type of app. However, no effects were found from type of app and type of review on users´ privacy concerns and privacy risk perception. Thus, as expected from existing research, this demonstrates that users are not able to make inferences about possible privacy and security risks based on the type of app or type of review they are confronted with. The findings of this study indicate that consumers are increasingly concerned about their personal information. Correspondingly, the general privacy attitude was found to be the predominant factor that influences users´ privacy concerns, risk perceptions and download intentions. It is therefore of great importance to increase users' perception of safety by assuring that their personal information is treated confidentially in order to increase trust and decrease risk perception.

References

Ackerman, M. S., Cranor, L. F., & Reagle, J. (1999, November). Privacy in e-commerce: examining user scenarios and privacy preferences. In *Proceedings of the 1st ACM conference on Electronic commerce* (pp. 1-8). ACM

Agius, A. (2014). Unbelievable Mobile Marketing Success Stories. Retrieved from: http://www.business2community.com/mobile-apps/7-unbelievable-mobile-marketing-success-stories-0808211

Ahluwalia, R., Burnkrant, R. E., & Unnava, H. R. (2000). Consumer response to negative publicity: The moderating role of commitment. *Journal of Marketing Research, 37*(2), 203-214.

Ahmad, N. (2012). Utilitarian and Hedonic Values of Mobile Services: A Preliminary Analysis from the Users' Perspective. *Business & Accounting Review*, *9*, 69-83.

Ajzen, I. (1985). *From intentions to actions: A theory of planned behavior* (pp. 11-39). Berlin and Heidelberg: Springer.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Processes, 50,* 179-211.

Ajzen, I., & Fishbein, M. (1977). Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychological Bulletin*, *84*(5), 888.

Akturan, U., & Tezcan, N. (2012). Mobile banking adoption of the youth market: Perceptions and intentions. *Marketing Intelligence & Planning*, *30*(4), 444-459.

Alnawas, I., & Aburub, F. (2016). The effect of benefits generated from interacting with branded mobile apps on consumer satisfaction and purchase intentions. *Journal of Retailing and Consumer Services*, *31*, 313-322.

Andrade, E. B., Kaltcheva, V. & Weitz, B. (2002). Self-Disclosure on the Web: The Impact of Privacy Policy, Reward, and Company Reputation. *Advances in Consumer Research*, *29*(1), 350 – 353.

Android Authority. (2016). Android App permissions explained - Android Authority. Retrieved from http://www.androidauthority.com/android-app-permissions-explained-642452/

Android Developers. (2016). Manifest. Permission. Retrieved from https://developer.android.com/reference/android/Manifest.permission.html

Androidcentral. (2014, June 24). What some of those scary application permissions mean | Android Central. Retrieved from http://www.androidcentral.com/look-application-permissions

Ba, S., & Pavlou, P. A. (2002). Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. *MIS Quarterly*, 243-268.

Baber, A., Thurasamy, R., Malik, M. I., Sadiq, B., Islam, S., & Sajjad, M. (2016). Online word-of-mouth antecedents, attitude and intention-to-purchase electronic products in Pakistan. *Telematics and Informatics*, *33*(2), 388-400.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management*, *53*(1), 1-21.

Barkhuus, L., & Dey, A. K. (2003, July). Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns. In *Interact*, Vol. 3, pp. 702-712.

Barrera, D., Kayacik, H. G., van Oorschot, P. C., & Somayaji, A. (2010, October). A methodology for empirical analysis of permission-based security models and its application to android. In *Proceedings of the 17th ACM conference on Computer and communications security* (pp. 73-84). ACM.

Bauer, H. H., Reichardt, T., Barnes, S. J., & Neumann, M. M. (2005). Driving consumer acceptance of mobile marketing: A theoretical framework and empirical study. *Journal of Electronic Commerce Research*, *6*(3), 181.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, *11*(3), 245-270.

Bellman, S., Potter, R. F., Treleaven-Hassard, S., Robinson, J. A., & Varan, D. (2011). The effectiveness of branded mobile phone apps. *Journal of Interactive Marketing*, *25*(4), 191-200.

Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A., & Möller, S. (2011, August). On the need for different security methods on mobile phones. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services* (pp. 465-473). ACM

Benenson, Z., & Reinfelder, L. (2013, July). Should the users be informed? On differences in risk perception between android and iphone users. In *Symposium on Usable Privacy and Security (SOUPS)* (pp. 1-2).

Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*, *53*, 419-426.

Camarero, C., & San José, R. (2011). Social and attitudinal determinants of viral marketing dynamics. *Computers in Human Behavior*, *27*(6), 2292-2300.

Cheema, A., & Papatla, P. (2010). Relative importance of online versus offline information for Internet purchases: Product category and Internet experience effects. *Journal of Business Research*, *63*(9), 979-985.

Chen, Y. C., Shang, R. A., & Lin, A. K. (2009). The intention to download music files in a P2P environment: Consumption value, fashion, and ethical decision perspectives. *Electronic Commerce Research and Applications, 7*(4), 411-422. http://dx.doi.org/10.1016/j.elerap.2008.02.001

Cheng, J. M. S., Wang, E. S. T., Lin, J. Y. C., & Vivek, S. D. (2009). Why do customers utilize the internet as a retailing platform: A view from consumer perceived value. *Asia Pacific Journal of Marketing and Logistics, 21*(1), 144-160. http://dx.doi.org/10.1108/13555850910926290

Cheung, C. M., & Thadani, D. R. (2010). The effectiveness of electronic word-of-mouth communication: A literature analysis. *Proceedings of the 23rd Bled eConference eTrust: implications for the individual, enterprises and society*, 329-345.

Cheung, C. M., & Thadani, D. R. (2012). The impact of electronic word-of-mouth communication: A literature analysis and integrative model. *Decision Support Systems*, *54*(1), 461-470.

Chia, P. H., Yamamoto, Y., & Asokan, N. (2012, April). Is this app safe?: a large scale study on application permissions and risk signals. In *Proceedings of the 21st international Conference on World Wide Web* (pp. 311-320). ACM.

Chiu, C. M., Wang, E. T., Fang, Y. H., & Huang, H. Y. (2014). Understanding customers' repeat purchase intentions in B2C e-commerce: the roles of utilitarian value, hedonic value and perceived risk. *Information System Journal, 24*(1), 85-114.

Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annu. Rev. Psychol.*, *55*, 591-621.

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012, July). Measuring user confidence in smartphone security and privacy. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (p. 1). ACM.

Choe, E. K., Jung, J., Lee, B., & Fisher, K. (2013, September). Nudging people away from privacy-invasive mobile apps through visual framing. In *IFIP Conference on Human-Computer Interaction* (pp. 74-91). Berlin and Heidelberg: Springer.

Cranor, L. F., Guduru, P., & Arjula, M. (2006). User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction (TOCHI)*, *13*(2), 135-178.

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

Culnan, M. J. (1993). "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. *MIS quarterly*, 341-363.

Cunningham, S. M. (1967). The major dimensions of perceived risk. *Risk taking and information handling in consumer behavior*, *1*, 82-111.

Dhar, R., & Wertenbroch, K. (2000). Consumer choice between hedonic and utilitarian goods. *Journal of marketing research*, *37*(1), 60-71.

Doh, S. J., & Hwang, J. S. (2009). How consumers evaluate eWOM (electronic word-of-mouth) messages. *CyberPsychology & Behavior*, *12*(2), 193-197.

Doney, P. M., & Cannon, J. P. (1997). An examination of the nature of trust in buyer-seller relationships. *The Journal of Marketing*, 35-51.

Dooley, D. (2001). *Social research methods*. Upper Saddle River (N.J.): Prentice Hall.

Dooley, D., & Vos, H. J. (2008). *Social research methods*. Harlow: Pearson Custom Publ.

Eling, N., Krasnova, H., Widjaja, T., & Buxmann, P. (2013). Will you accept an app? Empirical investigation of the decisional calculus behind the adoption of applications on Facebook. *Proceedings of the 34th International Conference on Information Systems*, 1-30.

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.

Felt, A. P., Greenwood, K., & Wagner, D. (2011, June). The effectiveness of application permissions. In *Proceedings of the 2nd USENIX Conference on Web Application Development (WebApps)*, 2011.

Festinger, L. (1957). *A Theory of cognitive dissonance*. Stanford, CA: Stanford University Press.

Field, A. (2013). *Discovering statistics using IBM SPSS statistics*. Sage.

Fife, E., & Orjuela, J. (2012). The privacy calculus: Mobile apps and user perceptions of privacy and security. *International Journal of Engineering Business Management*, *4*.

Filieri, R. (2015). What makes online reviews helpful? A diagnosticity-adoption framework to explain informational and normative influences in e-WOM. *Journal of Business Research*, *68*(6), 1261-1270.

Finlay, K. A., Trafimow, D., & Moroi, E. (1999). The importance of subjective norms on intentions to perform health behaviors. *Journal of Applied Social Psychology*, *29*(11), 2381-2393.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, Mass.: Addison-Wesley.

Friedman, B., Khan Jr, P. H., & Howe, D. C. (2000). Trust online. *Communications of the ACM*, *43*(12), 34-40.

Fu, B., Lin, J., Li, L., Faloutsos, C., Hong, J., & Sadeh, N. (2013, August). Why people hate your app: Making sense of user feedback in a mobile app store. In *Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining* (pp. 1276-1284). ACM.

Gervey, B., & Lin, J. (2000). The age factor: how internet use varies from teens to seniors. *Advertising Age*, *71*(16), 22.

Google Play. (2016). Review app permissions thru Android 5.9 - Google Play Help. Retrieved from https://support.google.com/googleplay/answer/6014972?hl=en

Google Play Store. (2016). Control your app permissions on Android 6.0 and up - Google Play Help. Retrieved from https://support.google.com/googleplay/answer/6270602?hl=en

Google Play Store. (2016). Review app permissions thru Android 5.9 - Google Play Help. Retrieved from https://support.google.com/googleplay/answer/6014972?hl=en

Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: Consumers' awareness and concerns. *Journal of Consumer Marketing*, *19*(4), 302-318.

Grazioli, S., & Jarvenpaa, S., (2000). Perils of Internet fraud: an empirical investigation of deception and trust with experienced Internet consumers. *IEEE Transactions on Systems, Man, and Cybernetics 30*(4), 395 – 410.

Gu, J., Xu, Y. C., Xu, H., Zhang, C., & Ling, H. (2016). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*.

Gumroad.com. (2015). *The Mobile App Experience - Uncovering the consumer journey from app discovery to loyalty*. Retrieved from https://gumroad.com/l/usMobileAppExperience/

Hann, I. H., Hui, K. L., Lee, T., & Png, I. (2002). Online information privacy: Measuring the cost-benefit trade-off. *ICIS 2002 Proceedings*, 1.

Harman, M., Jia, Y., & Zhang, Y. (2012, June). App store mining and analysis: MSR for app stores. In *Proceedings of the 9th IEEE Working Conference on Mining Software Repositories* (pp. 108-111). IEEE Press.

Harris, M. A., Brookshire, R., & Chin, A. G. (2016). Identifying factors influencing consumers' intent to install mobile applications. *International Journal of Information Management*, *36*(3), 441-450.

Harris, M. A., Chin, A. G., & Brookshire, R. (2015). Mobile App Installation: the Role of Precautions and Desensitization. *Journal of International Technology and Information Management*, *24*(4), 3.

Harris, M. A., Brookshire, R., Patten, K., & Regan, B. (2015). Mobile Application Installation Influences: Have Mobile Device Users Become Desensitized to Excessive Permission Requests? In *Proceedings of the Twentieth Americas Conference on Information Systems (AMCIS 2015)* (pp. 13-15).

Hawthorn, D. (2000). Possible implications of aging for interface designers. *Interacting with computers*, *12*(5), 507-528.

Heider, F. (1958). *The psychology of interpersonal relations*. New York: Wiley.

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM*, *42*(4), 80-85.

Hofstede, G.J., Minkov, M., & Hofstede, G (2014). Allemaal andersdenkenden: omgaan met cultuurverschillen. Business Contact.

Hoon, L., Vasa, R., Schneider, J. G., & Grundy, J. (2013). An analysis of the mobile app review landscape: trends and implications. *Faculty of Information and Communication Technologies, Swinburne University of Technology, Tech. Rep*.

Hsin Chang, H., & Wen Chen, S. (2008). The impact of online store environment cues on purchase intention: Trust and perceived risk as a mediator. *Online information review*, *32*(6), 818-841.

Hsu, C. L., & Lin, J. C. C. (2015). What drives purchase intention for paid mobile apps?–An expectation confirmation model with perceived value. *Electronic Commerce Research and Applications*, *14*(1), 46-57.

Hsu, J. S. C., Lin, T. C., Fu, T. W., & Hung, Y. W. (2015). The effect of unexpected features on app users' continuance intention. *Electronic Commerce Research and Applications*, *14*(6), 418-430.

Iacob, C., Veerappa, V., & Harrison, R. (2013, September). What are you complaining about: a study of online reviews of mobile applications. In *Proceedings of the 27th International BCS Human Computer Interaction Conference* (p. 29). British Computer Society.

IKEA. (2016). Download IKEA apps - IKEA. Retrieved from http://www.ikea.com/ms/en_CN/customer_service/download-ikea-apps/index.html

Jacoby, J., & Kaplan, L. B. (1972). The components of perceived risk. In *SV-Proceedings of the third annual conference of the association for consumer research*.

Jarvenpaa, S.L., Tractinsky, N., 1999. Consumer trust in an Internet store: a cross-cultural validation. *Journal of Computer Mediated Communication 5*(2), 1 – 33.

Joinson, A. N., Reips, U. D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human–Computer Interaction*, *25*(1), 1-24.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the econometric society*, 263-291.

Kang, S. (2014). Factors influencing intention of mobile application use. *International Journal of Mobile Communications*, *12*(4), 360-379.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607-635.

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.

Kelley, P. G., Bresee, J., Cranor, L. F., & Reeder, R. W. (2009, July). A nutrition label for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (p. 4). ACM.

Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N., & Wetherall, D. (2012). A conundrum of permissions: Installing applications on an android smartphone. In *Financial Cryptography and Data Security* (pp. 68-79). Springer Berlin Heidelberg.

Kelley, P. G., Cranor, L. F., & Sadeh, N. (2013, April). Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 3393-3402). ACM.

Kennedy, A., & Inkpen, D. (2006). Sentiment classification of movie reviews using contextual valence shifters. *Computational intelligence*, *22*(2), 110-125.

Khalid, H., Shihab, E., Nagappan, M., & Hassan, A. E. (2015). What do mobile app users complain about? *IEEE Software*, *32*(3), 70-77.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision support systems*, *44*(2), 544-564.

Kim, H. W., Kankanhalli, A., & Lee, H. L. (2016). Investigating decision factors in mobile application purchase: A mixed-methods approach. *Information & Management*.

Kim, H. W., Lee, H. L., & Son, J. E. (2011, July). An exploratory study on the determinants of smartphone app purchase. In *The 11th International DSI and the 16th APDSI Joint Meeting, Taipei, Taiwan*.

Kim, J., Park, Y., Kim, C., & Lee, H. (2014). Mobile application service networks: Apple's App Store. *Service Business*, *8*(1), 1-27.

King, J. (2012). How Come I'm Allowing Strangers to Go Through My Phone? Smartphones and Privacy Expectations. *Smartphones and Privacy Expectations. (March 15, 2012)*.

Kleijnen, M., De Ruyter, K., & Wetzels, M. (2007). An assessment of value creation in mobile service delivery and the moderating role of time consciousness. *Journal of Retailing*, *83*(1), 33-46.

Koohikamali, M., & Kim, D. (2015). Does Information Sensitivity Make A Difference? Mobile Applications' Privacy Statements: A Text Mining Approach. In *Americas Conference on Information Systems, Puerto Rico*.

Krasnova, N. Eling, O. Abramova, and. Buxmann P (2014). Dangers of Facebook login for mobile apps: Is there a price tag for social information? *In Proceedings of the International Conference on Information Systems (ICIS).*

Laguna, K., & Babcock, R. L. (1997). Computer anxiety in young and older adults: Implications for human-computer interactions in older populations. *Computers in human behavior*, *13*(3), 317-326.

Lai, Y. L., Kuan, K. K., Hui, K. L., & Liu, N. (2009). The effects of moving animation on recall, hedonic and utilitarian perceptions, and attitude. *IEEE transactions on engineering management*, *56*(3), 468-477.

Lane, M. (2012, December). Does the android permission system provide adequate information privacy protection for end-users of mobile apps?. In *Proceedings of the 10th Australian Information Security Management Conference (SECAU 2012)* (pp. 67-74). Edith Cowan University, Security Research Institute.

Lee, M. C. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications*, *8*(3), 130-141.

Lee, H., Lim, D., Kim, H., Zo, H., & Ciganek, A. P. (2015). Compensation paradox: the influence of monetary rewards on user behaviour. *Behaviour & Information Technology*, *34*(1), 45-56.

Liang, Y. J. (2016). Reading to make a decision or to reduce cognitive dissonance? The effect of selecting and reading online reviews from a post-decision context. *Computers in Human Behavior*, *64*, 463-471.

Lifehacker. (2016). Why Does This Android App Need So Many Permissions? Retrieved from http://lifehacker.com/5991099/why-does-this-android-app-need-so-many-permissions

Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J., & Zhang, J. (2012, September). Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (pp. 501-510). ACM.

Liu, C. Z., Au, Y. A., & Choi, H. S. (2012). An empirical study of the freemium strategy for mobile apps: Evidence from the google play market.

Madden, T. J., Ellen, P. S., & Ajzen, I. (1992). A comparison of the theory of planned behavior and the theory of reasoned action. *Personality and Social Psychology Bulletin*, *18*(1), 3-9.

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

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: a trust building model. *The Journal of Strategic Information Systems*, *11*(3), 297-323.

McLeod, S. A. (2014). Cognitive Dissonance. Retrieved from www.simplypsychology.org/cognitive-dissonance.html

Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication*, (*9)*4.

Muslukhov, I., Boshmaf, Y., Kuo, C., Lester, J., & Beznosov, K. (2012, April). Understanding users' requirements for data protection in smartphones. In *Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference on* (pp. 228-235). IEEE.

Nam, C., Song, C., Lee, E., & Park, C. I. (2006). Consumers' privacy concerns and willingness to provide marketing-related personal information online. *Advances in Consumer Research*, *33*, 212.

Nowak, G. J., & Phelps, J. (1992). Understanding privacy concerns. An assessment of consumers' information-related knowledge and beliefs. *Journal of Direct Marketing*, *6*(4), 28-39.

Okazaki, S. (2009). Social influence model and electronic word of mouth: PC versus mobile internet. *International Journal of Advertising*, *28*(3), 439-472.

Pagano, D., & Maalej, W. (2013, July). User feedback in the appstore: An empirical study. In *Requirements Engineering Conference (RE), 2013 21st IEEE International* (pp. 125-134). IEEE.

Palka, W., Pousttchi, K., & Wiedemann, D. G. (2009). Mobile word-of-mouth–A grounded theory of mobile viral marketing. *Journal of Information Technology*, *24*(2), 172-185.

Palvia, P. (2009). The role of trust in e-commerce relational exchange: A unified model. *Information & management*, *46*(4), 213-220.

Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior*, *28*(3), 1019-1027.

Park, D. H., & Lee, J. (2009). E-WOM overload and its effect on consumer behavioural intention depending on consumer involvement. *Electronic Commerce Research and Applications*, *7*(4), 386-398.

Parker, R. G., & Parrott, R. (1994). Patterns of self-disclosure across social support networks: elderly, middle-aged, and young adults. *International Journal of Aging & Human Development*, *41*(4), 281-297.

Pavlou, P. A., & Chellappa, R. K. (2001). The role of perceived privacy and perceived security in the development of trust in electronic commerce transactions. *Marshall School of Business, USC, Los Angeles*.

PCWorld. (2011, February). Apple Hit With Another Suit Alleging Privacy Violations | PCWorld. Retrieved from http://www.pcworld.com/article/218351/article.html

Pennington, R., Wilcox, H. D., & Grover, V. (2003). The role of system trust in business-to-consumer transactions. *Journal of Management Information Systems*, *20*(3), 197-226.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, *19*(1), 27-41.

Racherla, P., Furner, C., & Babb, J. (2012). Conceptualizing the implications of mobile app usage and stickiness: A research agenda. *Available at SSRN 2187056*.

Rossi, L. (2010). Playing your network: gaming in social network sites. *Available at SSRN 1722185*.

Rouibah, K., Lowry, P. B., & Hwang, Y. (2016). The effects of perceived enjoyment and perceived risks on trust formation and intentions to use online payment systems: New perspectives from an Arab country. *Electronic Commerce Research and Applications*, *19*, 33-43.

Sarma, B. P., Li, N., Gates, C., Potharaju, R., Nita-Rotaru, C., & Molloy, I. (2012, June). Android permissions: a perspective combining risks and benefits. In *Proceedings of the 17th ACM Symposium on Access Control Models and Technologies* (pp. 13-22). ACM.

Sen, S., & Lerman, D. (2007). Why are you telling me this? An examination into negative consumer reviews on the web. *Journal of Interactive Marketing*, *21*(4), 76-94.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of public policy & marketing*, *19*(1), 62-73.

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014, April). Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems* (pp. 2347-2356). ACM.

Sjöberg, L., Moen, B. E., & Rundmo, T. (2004). *Explaining risk perception. An evaluation of the psychometric paradigm in risk perception research.* Trondheim.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, *35*(4), 989-1016.

Snacksafely.com. (2009). Barcode Scanning Apps: What They Don't Know CAN Hurt You | SnackSafely.com. Retrieved from http://snacksafely.com/2014/12/barcode-scanning-apps-what-they-dont-know-can-hurt-you/

123RF Stock photos. (2016). Cowpland #1 Royalty Free Photos, Pictures, Images and Stock Photography. Retrieved from http://www.123rf.com/profile_cowpland

Stone, R.N., & Gronhaug, K. (1993), "Perceived Risk: Further Considerations for the Marketing Discipline," *European Journal of Marketing*, Vol. 27, 3, 39-50.

Sweeney, J. C., Soutar, G. N., & Johnson, L. W. (1999). The role of perceived risk in the quality-value relationship: a study in a retail environment. *Journal of Retailing*, *75*(1), 77-105.

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.

Taylor, D. G., Davis, D. F., & Jillapalli, R. (2009). Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research*, *9*(3), 203-223.

TheVerge. (2012, February). iOS address book privacy: app developers and Apple respond | The Verge. Retrieved from http://www.theverge.com/2012/2/15/2800397/ios-apps-contents-privacy-permission

Wagner, N., Hassanein, K., & Head, M. (2010). Computer use by older adults: A multi-disciplinary review. *Computers in human behavior*, *26*(5), 870-882.

Wang,D.H.M.,Yu, T. H. K., & Chiang, C. H. (2015). Exploring the value relevance of corporate reputation: A fuzzy-set qualitative comparative analysis. *Journal of Business Research, 69*(4), 1329-1332.

Wang, H., Lee, M. K., & Wang, C. (1998). Consumer privacy concerns about Internet marketing. *Communications of the ACM*, *41*(3), 63-70.

Wang, H. Y., Liao, C., & Yang, L. H. (2013). What affects mobile application use? The roles of consumption values. *International Journal of Marketing Studies*, *5*(2), 11.

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management, 36*(4), 531-542.

Wang, Y., & Wang, K. L. (2008). THE INFLUENCE OF INFORMATION SENSITIVITY, COMPENSATION ON PRIVACY CONCERN AND BEHAVIOUR INTENTION. *PACIS 2008 Proceedings*, 112.

Wang, Y., Zheng, J., Sun, C., & Mukkamala, S. (2013, July). Quantitative security risk assessment of android permissions and applications. In *IFIP Annual Conference on Data and Applications Security and Privacy* (pp. 226-241). Berlin and Heidelberg: Springer.

Weinberger, M. C., & Dillon, W. R. (1980). The effects of unfavorable product information. *Advances in Consumer Research* 7,. 528–532.

Westin, A. (1967). *The right to privacy*. New York: Athenaeum.

Wiedemann, D. G., Palka, W., & Pousttchi, K. (2009). Business models for mobile payment service provision and enabling. *Mobile and Ubiquitous Commerce: Advanced E-Business Methods*, 29-47.

Woo, J. (2006). The right not to be identified: privacy and anonymity in the interactive media environment. *New media & Society*, *8*(6), 949-967.

Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, *28*(3), 889-897.

Xiang, J. Y., Jing, L. B., Lee, H. S., & Choi, I. Y. (2015). A comparative analysis on the effects of perceived enjoyment and perceived risk on hedonic/utilitarian smartphone applications. *International Journal of Networking and Virtual Organisations*, *15*(2-3), 120-135.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, *51*(1), 42-52.

Yang, S., & Wang, K. (2009). The influence of information sensitivity compensation on privacy concern and behavioural intention. *ACM SIGMIS Database*, *40*(1), 38-51.

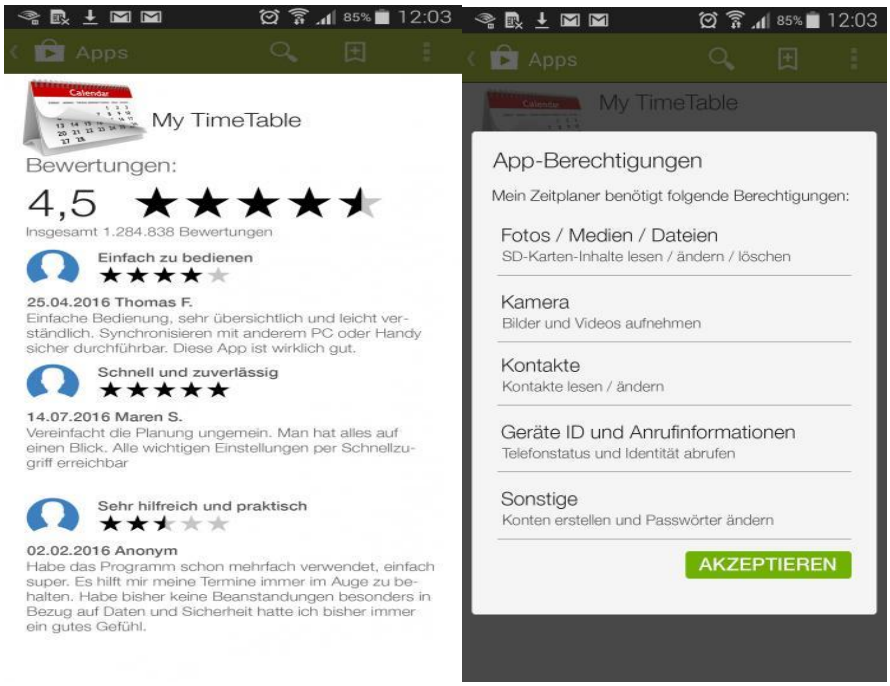
Yang, H., Zhou, L. (2011). Extending TPB and TAM to mobile viral marketing: An exploratory study on American young consumers' mobile viral marketing attitude, intent and behavior, *Journal of Targeting, Measurement and Analysis for Marketing, 19*(2), 85-98.

Appendices

Appendix A Scenarios used in the study

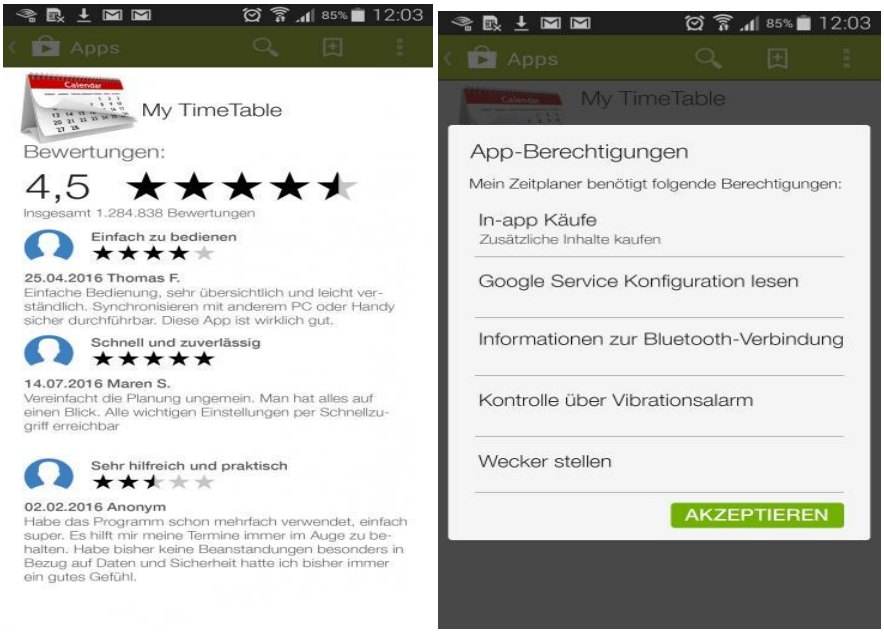
Scenario 1

Type of app: utilitarian, Type of permission: high sensitive, Type of review: positive review and ratings



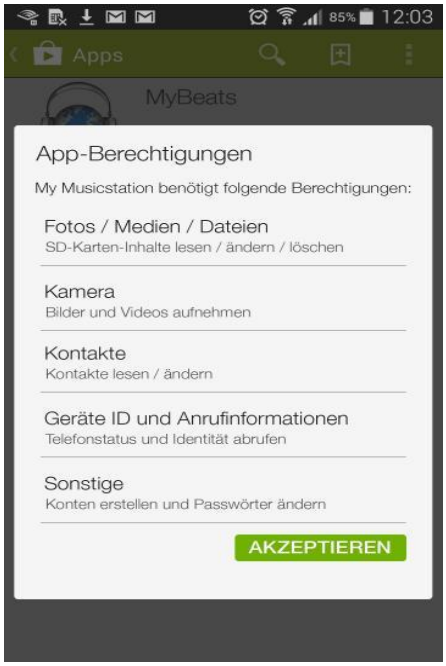
Scenario 2

Type of app: utilitarian, Type of permission: low sensitive, Type of review: positive review and ratings



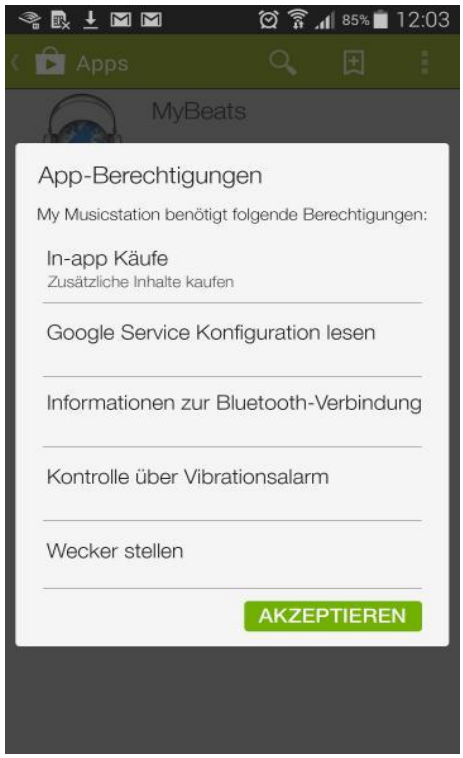
Scenario 3

Type of app: hedonic, Type of permission: high sensitive, Type of review: positive review and ratings



Scenario 4

Type of app: hedonic, Type of permission: low sensitive, Type of review: positive review and ratings

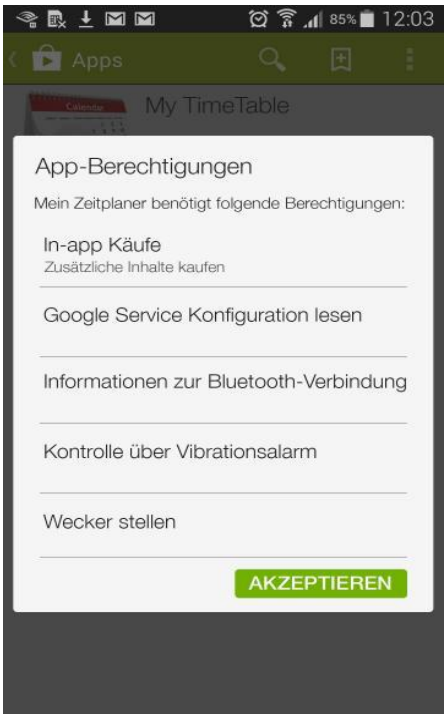


Scenario 5

Type of app: utilitarian, Type of permission: high sensitive, Type of review: negative review and ratings

Scenario 6

Type of app: utilitarian, Type of permission: low sensitive, Type of review: negative review and ratings



Scenario 7

Type of app: hedonic, Type of permission: high sensitive, Type of review: negative review and ratings

Scenario 8

Type of app: hedonic, Type of permission: low sensitive, Type of review: negative review and ratings

Appendix B Survey

Original Survey in German

Introduction

Liebe/r Teilnehmer/in,

Willkommen zum Abschlussprojekt meiner Masterarbeit Vielen Dank, dass Sie sich die Zeit nehmen um an der Umfrage die sich mit dem Herunterladen von mobilen Apps und deren Zugangsberechtigungen beschäftigt, teilzunehmen.

Ihre Teilnahme wird mir helfen mein Master Studium im Bereich Marketing Kommunikation an der Universität Twente erfolgreich abzuschließen. Die Umfrage wird nicht mehr als 5-10 Minuten Ihrer Zeit in Anspruch nehmen und kann jederzeit abgebrochen werden. Sie sollte jedoch wenn möglich in einem Durchgang durchgeführt und ehrlich beantwortet werden. Ihre Meinung ist wichtig, es gibt kein Richtig oder Falsch.

Die Ergebnisse der Umfrage sind anonym und werden ausschließlich für akademische Forschungszwecke benutzt. Bei eventuellen Rückfragen und Anmerkungen können Sie mich gerne unter folgende e-mail kontaktieren: s.beckmann@student.utwente.nl

Im Folgenden werden Sie nun einen Text einer angebotenen App sehen. Bitte lesen Sie diesen nun aufmerksam und beantworten die darauf folgenden Fragen.

Mit freundlichen Grüßen,

Svenja Beckmann

Student Marketing Kommunikation, Universität Twente

Klicken Sie nun auf die Einverständniserklärung um die Umfrage zu starten.

❍ Ich erkläre mich bereit freiwillig an der Umfrage teilzunehmen (1)

Demographics

Was ist ihr Geschlecht?

❍ männlich (1)
❍ weiblich (2)

Wie alt sind Sie?

- ❍ unter 20 Jahre (1)
- ❍ 20 - 29 Jahre (2)
- ❍ 30 - 39 Jahre (3)
- ❍ 40 - 49 Jahre (4)
- ❍ 50 - 59 Jahre (5)
- ❍ 60 - 69 Jahre (6)
- ❍ 70 - 79 Jahre (7)
- ❍ über 80 Jahre (8)

106 Welchen höchsten Bildungsabschluss haben Sie?

- ❑ Keinen Abschluss (1)
- ❑ Mittlerer Schulabschluss (2)
- ❑ Berufsausbildung (3)
- ❑ Abitur oder Fachabitur (4)
- ❑ Bachelorabschluss oder vergleichbar (5)
- ❑ Masterabschluss oder vergleichbar (6)
- ❑ Doktortitel (7)
- ❑ Anderer, nämlich (8) _____

Bitte geben Sie an mit welchem mobilen Gerät sie Apps nutzen. Mehrere Antworten sind möglich.

- ❑ Handy (1)
- ❑ Tablet (3)
- ❑ Computer (Laptop) (4)
- ❑ Andere, nämlich (5) _____

Welches Betriebssystem hat Ihr Telefon?

- ❍ Android (1)
- ❍ iOS (2)
- ❍ Windows (3)
- ❍ andere, nämlich (4) _____

Welche Kategorie mobiler Apps nutzen Sie am meisten? Mehrere Antworten sind möglich.

- ❑ Spiele (1)
- ❑ Unterhaltung (z. B. Musik, Filme, Sport, TV) (2)
- ❑ Werkzeuge (z. B. Navigation, Rechner, Taschenlampe, QR Reader, Barcode Scanner) (3)
- ❑ Soziale Netzwerke (z. B. Facebook, Twitter, Instagram) (4)
- ❑ Messenger (Whats App, Facebook , MSN) (5)
- ❑ Gesundheit (z. B. Fitness, Ernährung) (6)
- ❑ Informationen (z. B. News, Wetter, Lifestyle) (7)
- ❑ Geld/Finanzen (z. B. Online Banking, Paypal etc.) (8)
- ❑ Produktivität (z. B. Kalender, Notizen, E-mail, PDF-Reader, Office Tools) (9)
- ❑ sonstige, nämlich (10) _____

Bitte geben Sie auf einer Skala von 1 (trifft nicht zu) bis 5 (trifft zu), wie sehr sie mit den folgenden Aussagen übereinstimmen.

	Trifft nicht zu (1)	Trifft eher nicht zu (2)	Teils-Teils (3)	Trifft eher zu (4)	Trifft zu (5)
Für mich ist das Wichtigste, dass meine Informationen privat bleiben (1)	❍	❍	❍	❍	❍
Verglichen mit anderen bin ich eher um die Gefahren besorgt, die meine Privatsphäre bedrohen (2)	❍	❍	❍	❍	❍
Ich finde es wichtig, dass ich die Kontrolle darüber habe wer meine persönlichen Informationen benutzen kann (3)	❍	❍	❍	❍	❍
Ich bin davon überzeugt, dass meine Privatsphäre respektiert und geschützt werden sollte. (4)	❍	❍	❍	❍	❍

Welche der folgenden Produkte haben sie kürzlich schon mal online gekauft?

- ❑ Kleidung (1)
- ❑ Schuhe (2)
- ❑ Bücher (3)
- ❑ Elektronische Artikel (4)
- ❑ Musik (5)
- ❑ Reisen (6)
- ❑ Möbel (7)
- ❑ Haushaltwaren (8)
- ❑ Gartenzubehör (9)
- ❑ Sonstige, nämlich (10) _____

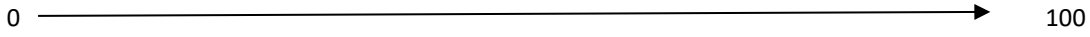
Beginn Scenarios

Stellen Sie Sich folgende Situation vor: Sie möchten eine App herunterladen auf ein mobiles Gerät wie z. B Smartphone, Android oder Tablet. Vor dem Download sehen sie auf dem Bildschirm zuerst die Bewertungen und Kommentare anderer Nutzer dieser App. Bitte lesen Sie die folgenden Informationen sorgfältig, um die darauffolgenden Fragen zu beantworten.

Nachdem Sie die Bewertungen anderer Nutzer dieser App gelesen haben werden sie nun aufgefordert den Zugangsberechtigungen zuzustimmen, um die App herunterzuladen und zu nutzen. Die geforderten Berechtigungen werden Ihnen nun auf dem Bildschirm angezeigt.

(Draggable bar Chart) Bitte geben Sie an wie sensibel Sie die gefragten Zugangsberechtigungen auf einer Skala von 0 (überhaupt nicht sensibel) bis 100 (extrem sensibel) beurteilen:

Sensibilität der Zugangsberechtigungen



(Draggable bar chart was recoded to a 5-point Likert scale for further analysis)

Wie würden Sie die allgemeinen Nutzerbewertungen der App beurteilen. Die Nutzerbewertungen der App sind:

	1	2	3	4	5
Negative(1) :Postiv (5)	❍	❍	❍	❍	❍

Kennen Sie die soeben gezeigte App?

❍ Ja (1)
❍ Nein (2)

Benutzen Sie zurzeit eine App dieser Art?

❍ Ja (1)
❍ Nein (2)

Bitte geben Sie auf einer Skala von 1 (trifft nicht zu) bis 5 (trifft zu), wie sehr sie mit den folgenden Aussagen über die präsentierte App übereinstimmen.

	Trifft nicht zu (1)	Trifft eher nicht zu (2)	Teils-Teils (3)	Trifft eher zu (4)	Trifft zu (5)
Dies ist eine App für die Organisation und Planung meines Alltags. (1)	❍	❍	❍	❍	❍
Diese App hilft mir meine Ziele effektiver zu erreichen (2)	❍	❍	❍	❍	❍
Diese App dient zur Unterhaltung (3)	❍	❍	❍	❍	❍
Diese App bereitet mir Vergnügen/Freude (4)	❍	❍	❍	❍	❍

Bitte geben Sie auf einer Skala von 1 (trifft nicht zu) bis 5 (trifft zu), wie sehr Sie mit den folgenden Aussagen übereinstimmen.

	Trifft nicht zu (1)	Trifft eher nicht zu (2)	Teils-Teils (3)	Trifft eher zu (4)	Trifft zu (5)
Ich bin besorgt darüber, dass Informationen die die App über mich sammelt missbraucht werden könnten (1)	❍	❍	❍	❍	❍
Ich bin besorgt über den Schutz meiner Privatsphäre beim Download dieser App. (2)	❍	❍	❍	❍	❍
Ich bin besorgt darüber, dass Informationen die die App über mich sammelt zu unvorhersehbaren Zwecken genutzt werden könnten (3)	❍	❍	❍	❍	❍

Bitte geben Sie basierend auf den gerade gezeigten Informationen über die App auf einer Skala von 1 (trifft nicht zu) bis 5 (trifft zu) an, wie sehr Sie mit den folgenden Aussagen übereinstimmen.

	Trifft nicht zu (1) (1)	Trifft eher nicht zu (2) (2)	Teils-Teils (3) (3)	Trifft eher zu (4) (4)	Trifft zu (5) (5)
Der Download dieser App birgt ein höheres Risiko als andere Apps (1)	❍	❍	❍	❍	❍
Der Download dieser App ist risikoreich (2)	❍	❍	❍	❍	❍
Der Download dieser App ist gefährlich (3)	❍	❍	❍	❍	❍
Der Download dieser App könnte finanzielle Verluste mit sich bringen (4)	❍	❍	❍	❍	❍
In Hinsicht auf den Download dieser App, bin ich besorgt, ob sie so funktioniert wie sie soll (5)	❍	❍	❍	❍	❍
In Hinsicht auf den Download dieser App, bin ich besorgt, ob die App fehlerfrei funktioniert (6)	❍	❍	❍	❍	❍
Ich bin besorgt darüber, dass sich durch den Download dieser App unautorisierte Parteien Zugriff auf meine persönlichen Daten verschaffen könnten (7)	❍	❍	❍	❍	❍
Ich bin besorgt, dass meine persönlichen Daten an Dritte weitergegeben werden könnten (8)	❍	❍	❍	❍	❍

Bitte geben Sie basierend auf den soeben gezeigten Informationen zu der App, auf einer Skala von 1 (trifft nicht zu) bis 5 (trifft zu) an, wie sehr Sie mit den folgenden Aussagen übereinstimmen.

	Trifft nicht zu (1)	Trifft eher nicht zu (2)	Teils-Teils (3)	Trifft eher zu (4)	Trifft zu (5)
Diese App erscheint mir vertrauenswürdig (1)	❍	❍	❍	❍	❍
Ich habe Vertrauen darin, dass diese App zu meinem besten Interesse/Vorteil handelt (2)	❍	❍	❍	❍	❍
Ich habe Vertrauen darin, dass diese App ethische und moralische Standards erfüllt. (3)	❍	❍	❍	❍	❍
Ich habe Vertrauen darin, dass diese App meine persönlichen Informationen nicht an Dritte weitergibt (4)	❍	❍	❍	❍	❍
Ich habe Vertrauen darin, dass diese App meine persönlichen Informationen nicht an Dritte weitergibt ohne meine explizite Zustimmung (5)	❍	❍	❍	❍	❍
Ich habe Vertrauen darin, dass diese App ihre Funktionen erfüllt. (6)	❍	❍	❍	❍	❍

Bitte geben Sie basierend auf den soeben gezeigten Bewertungen der App an, wie Sie auf einer Skala von 1 (trifft nicht zu) bis 5 (trifft zu), mit den folgenden Aussagen übereinstimmen.

	Trifft nicht zu (1)	Trifft eher nicht zu (2)	Teils-Teils (3)	Trifft eher zu (4)	Trifft zu (5)
Ich werde nicht zögern diese App herunterzuladen (1)	❍	❍	❍	❍	❍
Die Wahrscheinlichkeit dass ich diese App herunterlade ist hoch (2)	❍	❍	❍	❍	❍
Ich werde sehr wahrscheinlich diese App umgehend herunterladen (3)	❍	❍	❍	❍	❍
Ich beabsichtige diese App umgehend herunterzuladen (4)	❍	❍	❍	❍	❍

Bitte geben Sie auf einer Skala von 1 (trifft nicht zu) bis 5 (trifft zu), wie sehr sie mit den folgenden Aussagen übereinstimmen.

	Trifft nicht zu (1)	Trifft eher nicht zu (2)	Teils-Teils (3)	Trifft eher zu (4)	Trifft zu (5)
Ich würde diese App meinen Freunden/Familie empfehlen (1)	❍	❍	❍	❍	❍
Ich würde positive Dinge über diese App sagen (2)	❍	❍	❍	❍	❍
Wenn meine Freunde/Familie eine App dieser Art suchen würden, würde ich ihnen diese App empfehlen (3)	❍	❍	❍	❍	❍

Appendix C Explanations of Permissions Used

Below the permissions used in the study are explained. The given explanations are adopted from information of the Google Play Store and Android Support (see references).

High sensitive permissions used

1. **Photos/Media/Files** (Read/change/delete contents on SD card)
   The app can use files and data stored on the device, read contents of storage (USB and SD card), modify or delete contents of the storage, format external storage, mount or unmount external storage
2. **Camera** (take pictures and videos)
   The app can use camera of the device by taking pictures and videos or record videos
3. **Contacts** (read/change)
   App can use contacts on the device and possibly read or modify them
4. **Device ID und call information** (phone status and Identity)
   The app can access the device ID, phone number, read phone status and identity
   it can use phone or call history, app may be able to directly call numbers (loss of money), read call log, modify phone state, make calls without owners' intervention, reroute outgoing calls
5. **Others (Create accounts and change passwords)**
   The app can use custom settings provided by the device manufacturer, read social stream (on some social networks), write to your social stream (on some social media networks), and access subscribed feeds

Low sensitive permissions used

1. **In-app purchases** (buy additional contents)
   The app can ask user to make purchases inside the app, often necessary for games
2. **Read Google Service configurations**
   The app can read sensitive log data, retrieve system internal state, read bookmarks and history, and retrieve running apps
3. **Information about Bluetooth-Connection**
   The app can control the Bluetooth on the device, including broadcasting or getting information about nearby Bluetooth devices
4. **Control vibrate mode**
   Allows access to the vibrator of the mobile device
5. **Set-alarm clock**
   The app can access or set alarm on the phone of the user or broadcast an intent to set an alarm for the user