# Factors influencing risk perceptions and download intention in the context of mobile Apps

Master Thesis Communication Science
Lena Lindemeier (s1625608)

UNIVERSITY OF TWENTE.

# Factors influencing risk perceptions and download intention in the context of mobile Apps

Master Thesis Communication Science

Master Marketing & Communication

Faculty Behavioural Science

University of Twente

Graduation committee:

1 st supervisor: Dr. Ardion Beldad

2 nd supervisor: Dr. Joyce Karreman

**Abstract**

The influence of mobile apps is steadily rising and so are the risks and uncertainties involved in the download process. These risks refer especially to privacy, including a lack of control about how personal data accessed by an app are handled. Since there is a research gap in this field, the purpose of this study was to investigate the influence of familiarity, recommendations with different sources and valences and the sensitivity of the permissions required by the app. In order to investigate these effects a survey was conducted with 285 participants from Germany. In the survey participants were exposed to eight different scenarios leading them through a download process in which the variables were manipulated.

The results of the study show that familiarity only influences people's technical risk perception but does not help to reduce their privacy concerns or general risk perception. Especially, the sensitivity of the permissions required by an app has an influence on privacy risk and general risk perception. Furthermore, it was shown that participants in the study had a high valuation towards their privacy, which was found to have an effect on people's risk perceptions as well as their download intention.

Based on the results, it was shown that people need to be given assurance about their privacy protection during the download process in order to address their sceptical attitude and their concerns. There is a special need for further research into the underlying mechanisms in app download decisions and factors influencing people's privacy concerns.

**Key words:**App download behaviour, mobile apps privacy risk, general risk perception, download intention, familiarity, app permissions, sensitivity, reviews

# Table of contents

## 1. Introduction:

The number of smartphone users has been steadily rising in recent years and with it also the use of mobile phone applications (apps). Apps were originally designed for organization- and information-related purposes, thus mainly including e-mail services, news, weather information or supporting users' general contact and time management (Hsu & Ling, 2015). The use of apps is steadily growing and so is the variety of them. Android users have a choice between approximately 1.6 million apps and Apple offers around 1.5 million different apps in the app store (Statista, 2016). People can now choose from a wide selection of apps including categories such as social media, health and fitness, games, lifestyle or general entertainment. The Mobile Behaviour Report (2014) states that 85% of users see their smartphone as an essential part of their everyday life. The study of Gupta (2013) adds that 82% of the time that people spend with their phone consists of app usage. In 2015 the total app downloads consisted of 25 million apps downloaded in Apple stores and 50 billion apps downloaded in the android app stores (Business of Apps, 2015)

Apps generated a turnover of approximately 41.1 billion dollars in 2015. These numbers are expected to rise to 101 billion in 2020 (Statista, 2016). These findings highlight the fact that apps have become a growing field offering opportunities to companies to expand their businesses, but also raises new questions for researchers with regards to the download behaviour of consumers. From a managerial point of view the influential factors with regards to users' risk perception and download intention are of essence. They serve them as an important source of information in order to be able to raise the download numbers of an app and adapt the general strategy.

In addition to the various benefits that apps offer to consumers, like entertainment or easy information search, there are also risks and uncertainties involved. Specifically, the protection of personal data can be at risk when downloading an app. Companies have an interest in user information in order to for example be able to match their advertisements more effectively to users (Olenski, 2013). Privacy concerns are especially present in the online environment, where in order to complete a transaction it is often necessary to provide a variety of personal information (Ermakova et al., 2014). Hence before being able to download an app, whether it is free or not, people are asked to share personal data and provide access to, for example, their information about their identities or locations. This means that disclosing data is a condition to successfully download an app. Since there are no direct borders in the online environment, insecurities about privacy occur. The growth of databases and the increasing amount of consumers' private information being collected, increase the risk for violating consumers' privacy and a loss of control in general (Culnan, 1993).

Since these concerns can be assumed to have a negative influence on people's intention to download an app, this study aims at examining the influences that can help to reduce these uncertainties among users. One influential factor in the context of app downloads may be familiarity. Hence, being familiar with an app or the company behind it might play a role with reference to people's willingness to download an app. Research highlights in particular the relation between familiarity and trust. Gefen (2000) states that familiarity helps people to reduce complexity and uncertainty and can be a decisive factor in their purchase decision, in this case for downloading an app.

Furthermore, social influence may be a factor that could sway people's willingness to download an app and affect their privacy concerns towards the download process (Rogers, 2003). There are different types of social influence. One type is in the form of recommendations by people who are in close relationship with the person, such as friends and family. In a survey it was shown that 52% learn about new apps from people within their close environment: their friends, peers or family (Benjamin, 2015). Furthermore, it was shown that this kind of word of mouth is seen as the most trusted source, with reference to purchase decisions, or in this case download decisions. In addition, electronic word

of mouth (eWOM) often serves as an influential factor. EWOM involves all kind of product related information, without commercial background that is spread via online channels, like online reviews (Litvin et al., 2008). An important difference is that in this case the opinion about the app comes from a stranger.

The goal of this study is therefore to examine the strength of the influence of both sources, if they are combined and provide contradictory information. Research on the influencing factors on download behaviour is limited. So far research mostly focuses on the influencing factors in e-commerce, this is why this research aims at closing this research gap. Research on app downloads so far have examined the influence of familiarity, sensitivity of permissions and different types of reviews- individually or combined with other different factors. Hence, the combination of the factors is chosen since it has not been examined so far. This study aims at closing this research gap.

Another aspect that is required for downloading an app, is to agree to the permissions that allow the app to access information or control functions on the smartphone. When agreeing with the permissions, the consumer provides access to for example his personal data or allows the app to control different functions as for example the Bluetooth connection (Glover et al., 2012). The permissions required for an app can also serve as an indicator for the risk that might be involved in the download process (Bonneau et al., 2009). Especially, the sensitivity of the data access required may have an influence on user's attitude towards the app and their download decision (Pan & Zinkhan, 2006).

The aim of this study is to provide additional information regarding the influential factors of people's willingness to download an app and their privacy concerns and risk perception in this context. An experimental study is going to be conducted in order to answer the following research questions:

**RQ**: **To what extent do familiarity, the sensitivity of the access required and recommendations from two sources with different valences have an influence on consumer's intention to download, their privacy risk and general risk perception?**

This research paper is structured as follows: Firstly, the theoretical framework background is presented including prior research concerning privacy concerns and the willingness to download an app as well as the potential influential factors, length of privacy statement, familiarity and social influence. Then the research model is presented followed by the methodology.

## 2. Theoretical framework

Apps offer users a wide range of possibilities, as they help them to organize their daily lifes, to plan their vacation or provide them with entertainment. However, when downloading an app there are several uncertainties involved. Apps often collect users' information and personal data, which means that there are uncertainties about how these sensitive data will be handled. Furthermore, there may be uncertainties, about the proper functioning or other technical aspects involved. The potential risks involved in the download process of an app are going to be discussed in the following.

### 2.2. General risk perception

Research, in the context of mobile applications and general online transactions, defines general risk as a feeling of uncertainty about the potential negative consequences of the download or online transaction (Featherman & Pavlou, 2003; Featherman & Wells, 2004). Dowling and Staelin (1994) add that it involves the perceived uncertainty and the potential occurrence of negative consequences, which involve financial aspects, as well as, for example privacy or social aspects. As previously mentioned, consumers are confronted with numerous risks when they download an app. Since downloading an app involves various uncertainties, consumers' perception of the general risk involved is an influential factor for the actual download decision.

General risk, with reference to downloading an app, can involve several aspects. Fortsythe and Shi (2003) found these aspects to be financial risk, technical risk, which is related to the product performance, as the most prominent risks for downloading an app. Smith, Milber and Burke (1996) add that unauthorized secondary use and improper access are common risks in the context of app downloads. The general risk perception of a person is an important variable because it can prevent people from building a positive attitude towards an app (Kim, Ferrin, & Rao, 2008). This can then have a negative influence on the adoption of an app and people's willingness to provide access to personal information (Featherman & Pavlou, 2003). Furthermore, Kim et al. (2008) point out that in the context of online shopping, perceived risk negatively influences people's purchase intention. It can thus be assumed that in the context of app downloads perceived risk is influential for the download decision. In the current study, risk is treated as a multidimensional construct, which is why it can be expected that there is a further division in a later state of the study.

### 2.1. Privacy Risk

There is one aspect in the context of risk perception that is of special importance: this is privacy risk. This is why privacy risk is going to be treated as a separate construct. The important nature of privacy risk, in the context of app downloading behaviour, is based on its prominence in the online environment. Hence, it is often necessary to provide access to a variety of personal information in order to complete the download process of an app (Ermakova et al., 2014). Milne, Rohm, and Bahl (2004) add that there are three risks that are strongly associated with online environment. These include the risk of unauthorized collection, the access to personal data, the transfer of personal data to third parties.

Privacy, in general, can be defined as people's prerogative to decide when, how and what kind of personal information is shared with others (Westin, 1967). People's personal definition of privacy can differ with reference to the situation they are in and the special needs attached to it. Westin (1966) divides these needs into four different categories: solitude, intimacy, anonymity and reserve. Especially the latter two aspects might be at risk when downloading an app. Mostly, it is not possible for people to stay anonymous and they lose the control over the kind of information they share, which is implied in Westin's term "reserve".

Concerns about people's privacy occur when they see their privacy to be at risk. Hence, when intending to download an app, whether or not the customer has to pay for it, he is asked to give access to his personal data in order to complete the download process. This process confronts the consumer with a lack of control because he has no direct control over the kind of information disclosed, the location where their data are saved and the way they are handled. These concerns have been found to negatively influence their trust in the app (Canfora et al., 2008). This may, therefore, influence consumers' decisions on whether or not to download an app. Privacy concerns are especially present in the online environment, where in order to complete a transaction it is often necessary to provide a array of personal information (Ermakova et al., 2014). This is also the case for mobile phone apps.

Privacy concerns mainly relate to the collection and tracking of data. Companies have a special interest in consumer information and location in order to, for example, personalize their services, to learn more about the desires and needs of their users and to increase the efficacy of their advertising. Although this does not necessarily involve bad intentions, people perceive it as a threat (Xu, Luo et al., 2011). By clicking on 'agree', consumers in some cases unknowingly also agree that their user data is forwarded to third parties; they use their data for personalized advertisements, which causes negative feelings among consumers (Felt et al.,2012). Also, research has shown that about 60% of smartphone users decided to not install an app based on the personal data that the app required (Pew Research, 2015).

### Privacy Paradox

Despite the fact that consumers feel threatened by the risk of data misuse when downloading an app, they keep on doing it. This can be seen as an example of the privacy paradox (Acquisti & Grossklags, 2005 ; Xu, Luo et al., 2011). King (2012), adds that although smartphone users store sensitive data on their devices, they do not take any action to protect their data. The privacy paradox in general describes the phenomenon as that although people state that they are concerned about their data and do not want to disclose personal information, they are willing to share that information in a real situation. The explanation given for this by the researchers is that the way people perceive risk and trust can differ, in imagined and in real situations. Xu, Luo et al. (2011) further state that the importance people attach to their data changes depending on the context. Hence, people might value their privacy more in a theoretical context than they do in real life.

### Privacy calculus

Wilson et al. (2012) point out that the concept of privacy calculus is a possible explanation for the privacy paradox. The privacy calculus can be defined as a cognitive process, in which the user weighs the potential benefits against the perceived risks involved in disclosing the personal data necessary for the app download (Min & Kim, 2015). Hence, the willingness to allow access to personal data depends on users' perceived risk or perceived benefits and which of both they perceive as dominant.

Although apps can evoke high risk perception and concerns among users, there are several factors that might influence their privacy risk perception, their general risk perception and eventually their download intention. In this study, three potential influences will be examined which are going to be discussed in the following.

### 2.3. Familiarity with the app:

In the process of downloading an app one of the first aspects that may be influential for the download decision is a person's familiarity with the app.

In psychology, familiarity is described as a subjective feeling of recognition, with reference to a situation, event, place, person or object (Psychology Dictionary, 2016). Referring to the familiarity with an app, it can therefore be referred to as whether a person has heard of the app and has a feeling of recognition or not.

There is a strong relation between familiarity and trust (Luhmann, 1979). Familiarity is an important factor for building trust, because it helps to create a comprehension of the environment in this case the app (Luhmann, 1979). Familiarity can also be related to past experience and can help to reduce concerns. Luhmann (1979) describes familiarity as experience and learning of how things work. In a later research Luhmann (1989) describes the importance of familiarity and trust in a technological context. He also points out the importance of familiarity for people's risk perception. In the research paper, Luhmann describes that people have two different ways of becoming familiar: firstly by directly using it or by reading about other users' experiences.

The research of Gefen (2000) states that familiarity helps people to reduce complexity and uncertainty and can be a decisive factor in a purchase decision. In his research he further states that familiarity serves as a mean to reduce uncertainty and towards a new technology. Mauldin and Arunachalam (2002) confirm that familiarity has a significant influence on purchase intention. Their research points out that familiarity has a positive effect on risk perception, because it helps to reduce the perceived transaction risk, the privacy concerns and general security risks. This indicates that consumers rate apps that they are familiar with as more secure. The study of Mollering (2006) adds that familiarity is an important factor for the building of trust which then helps to reduce general concerns. The research of Baumer (2004) adds that familiarity has a positive influence on people's willingness to provide personal information. Since the disclosure of personal information is necessary in the process of downloading an app it can therefore be assumed that familiarity may also have a positive influence on people's willingness to download an app. When people become familiar with an app their general concerns about privacy and risk are reduced, which then increases their willingness to disclose information or make a transaction (Slyke, Shim, Johnson & Jiang, 2006).

Thus far, research into the relationship between familiarity and purchase intention is mainly related to an e-commerce context. This is the reason why this research aims at examining the relationship in an app download context.

Li (2014) describes the aspect of familiarity that relates to people's knowledge or experience as the cognitive aspect of familiarity, adding that there is also an affective aspect which relates to feelings that familiarity can evoke. Studies also show that familiarity can evoke a feeling of intimacy among users (Lee & Kwon, 2011) which, according to Westin (2003), leads to a feeling of privacy. According to the researchers, a feeling of privacy positively influences people's willingness to disclose personal information, which is a condition for the intention to download an app. The cognitive aspect of familiarity helps people to reduce the privacy risk, which means that they assume that their privacy is more protected when they download a familiar app. Research states that familiarity does not mean that there are no potential risks, it helps to provide people with knowledge to deal with the potential risks or privacy concerns (Li, 2012). In addition to this, the research points out that the affective aspect of familiarity supports the consumer to build intimacy towards the app and to maintain this

relationship. This further helps the person to outbalance the potential risk and to reduce privacy concerns towards the download of an app.

Based on these theoretical findings, the following two hypotheses are assumed with reference to the influence of familiarity on people's privacy concerns and their willingness to download an app:

**H1: People confronted with a familiar app a) perceive lower privacy risk, b) perceive lower general risk ,c) have more trust in the app and d) have higher intention to download compared to people confronted with an unfamiliar app have**

## 2.4. Social influence

Before actually deciding to download an app, people are often confronted with various opinions about the app that might come from different types of sources. The Unified Theory of Acceptance and Use of Technology (UTAUT) states that in addition to perceived usefulness and the perceived ease of use, the social surrounding also has to be taken into account with regards to the adoption of technology (Venkatesh et al., 2003).

Social influence occurs when a person's behaviour, opinions or feelings are influenced by his social environment (Cialdini & Goldstein, 2004). Bagozzi and Dholakia (2002) state that people often do not adopt new technologies not because of their own preferences, but because of the opinions of others. Social influence can be divided into traditional word-of-mouth, which implies a source from the close environment, and electronic word-of-mouth, in which the source in a stranger. These two forms are going to be discussed in the following subsections.

### 2.4.1. Traditional word-of- mouth

Word-of-mouth (WOM) can be defined as a face-to-face communication between people about a product (Arndt, 1967). DiPietro et al. (2007) state that WoM is an influential factor for people's attitude towards a product. Furthermore, the researchers point out that it is the main source for decision-making. Godes and Mayzlin (2004) add that WOM can be considered one of the most essential forms of communication compared to other channels. It was also found that word-of- mouth helps consumers to reduce their perception of risks and therefore increases the potential willingness to download an app. Sen and Lermann (2007) add that this is the case because people trust those who are from their personal environment most. This is why traditional WOM was found to have a more positive influence on people than online reviews (Okdie et al., 2011).

Kelman (1974) divides social influence into three different forms. The first one is compliance, which describes the general agreement with others or the adoption of opinions (Kelman, 1958). With regards to the adoption of a new technology or app, this means that people might download an app if people from their social environment like it even -if they have shortage of information about it (Cheung et al., 2011). The second aspect is identification, which describes the fact that a person is influenced by others in their own social group (Cheung et al., 2011; Kelman, 1958). This involves an adoption of new technology as people want to keep a certain relationship with their social environment (Bagozzi & Lee, 2002). The third type is internalization, which involves accepting beliefs, opinions and behaviours because they are perceived as compatible with their own values (Kelman, 1958). In this case, the adoption of new technology is based on the fact that consumers see the technology in accordance with their own values (Cheung et al.,2010).

It was shown that there is a direct and an indirect form of social influence. The direct form includes the replication of experience. This means that people learn from the experience of their social environment, they adopt things that their social environments likes. This kind of decision making involves a lower risk perception because it relies on the judgement of others (Currie et al., 2008). According to the researchers the indirect form of social influence relies on the assumption that friends usually share the same preferences.

Rogers (2003) claims that for the adoption of new technology social influence is an important factor, especially via social networks. The researcher argues that subjective perceptions are, in this case, more valued than scientific or empirical facts.

Cialdini and Harpers (2009) state that the concept of social proof is one of the factors underlying social influence. The concept describes the fact that, especially in situations that are related to uncertainty, people have the general tendency to look at what people in their environment do. In relation to the download of an app, these uncertainties can be related to the potential risk and privacy concerns involved. In general, it can thus be assumed that the opinion of a close friend has an influence of people's perception of an app regarding their risk perception, their trust in the app and their actual willingness to download the app.

### 2.4.2. Electronic word-of-mouth

The increasing influence of the internet also has an impact on social influences. The internet offers consumers a great variety of opportunities, including new ways of communication. There is a shift from traditional WOM to electronic word-of-mouth (eWOM), which takes place online. Apps usually offer users the option to rate an app with the help of a star system (Pagano & Maalej, 2013) and add their personal opinion in a short statement. Before downloading an app, a potential user is confronted with the ratings of other users. The research organization Apptentive (2016) highlights the importance of those ratings. In their study they found that 90% of the people count the ratings of other users as a major influential factor in the decision of whether to download an app. Furthermore, their study points out that 50% of the participants do not even consider downloading an app if the star rating is three or less. As it was already described earlier, social influence -in this case eWOM- can influence people's general attitude towards an app regarding risk, trust or download intention. However, there is an important difference between the type of influence between traditional WOM and eWOM.

The difference between those two is the source. While in WOM the source is usually a person from the personal environment who has a rather close relationship to the person, the source of eWOM is mostly a stranger. Hence, there is a difference in the relationship between the reader of the review and the source. Lee et al. (2009) describes this relationship as "tie strength". The tie strength thus describes the closeness of an interpersonal relationship including factors as "emotional intensity, intimacy, amount of time or reciprocal service" (Granovetter, 1973, p.1361). According to Brown et al. (2007) there is a lack of person-to-person ties in eWOM, because of the fact that online communication is often anonymous.

The different relational strengths also have an influence on the credibility of a message. According to the research of Bansal et al. (2000), strong ties positively influence the credibility of a message. Meaning that if a recommendation comes from a close friend, it can be assumed that there is a higher influence on download intention compared with a recommendation from a strangers. The research of

Gilly et al. (1998) confirms that strong ties and the resulting credibility have persuasive power with reference to recommendations.

The aim of this study is to test the influence of recommendations of two different sources (friends vs strangers) on intention to download, privacy risk and general risk perception.

Since it was found that recommendations from people with a strong tie is in general perceived as more credible, the following hypotheses will be assumed for the study:

**H2 People confronted with a positive recommendation of a close friend and negative recommendations of strangers a) perceive lower privacy risk, b) perceive lower general risk c) have more trust in the app and d) have higher intention to download, compared with people confronted with a negative recommendation of a close friend and positive recommendations of strangers**

## 2.5. Sensitivity of permissions required

The last step before a user is able to download an app,is to agree with the permissions that the app requires. This means that the user is asked to give access to different types of data on their phones and to allow the app to operate certain functions of the smartphone. In comparison to other systems, Android provides the consumer with the largest amount of information regarding the permissions required to download an app (Kelley et al., 2011). The information about the permissions required is presented on a separate screen. When a consumer decides to download an app in the Android app store, there are two screens that are displayed to the consumer, the first one showing information about the app and the ratings of other users, the second one showing the actual permission screen (Glover et al., 2012).

According to Pew Research (2015) there are approximately 235 types of permissions that an app might require. Examples are: full network access, access to the microphone or access to photos, media and files. According to their research, the average number of permissions required by apps is five and point out that the largest number of permissions is needed for business and communication apps. The consumer has to agree with all the permissions required or otherwise is not able to download the app. Apps themselves do not automatically have the permission to carry out certain actions or to access data on a person's phone.

According to Pew Research Centre (2015) permissions can be described as developers' communication tool about how the app is going to interact with the user's smartphone and what kind of personal data is going to be accessed. After having provided the necessary permissions, an app is able to, for example, collect information about the users' location and movement, internet and social media habits and their photos, videos or contacts (Pew Research Centre, 2015). Also, some applications, for example, require the permission to send text messages, to access people's contacts or change settings like Bluetooth (Sarma et al., 2012). Hence, the function of a permission screen is to ask the consumer for permission to execute the functions necessary for the app. It was shown that one of the most required permissions is full internet access (Hornyack, 2011). According to Kelley et al. (2012) permission screens serve users as support to decide if they want to download an app or not. The consumer has to agree with all the permissions required or otherwise is unable to download the app. In their article, the reaserchers also state that permission screens are used as a means to protect people against malicious apps, by providing them with the opportunity to check which permissions are necessary for the app and let them decide themselves if they want to download it.

There are differences between the individual permissions required according to their perceived sensitivity. Hence, Sarma et al. (2012) state that the permissions an app requires can be considered as an indicator for the potential risk involved in downloading an app. Research showed that if people

perceive information requested to not be highly sensitive, they also perceive the involved risk to be lower than if information is perceived as sensitive (Pan & Zinkhan, 2006). Malhotra, Kim, and Agarwal (2004) confirm that when people perceive data required as very sensitive, the perceived risk increases which negatively influences people's willingness to give access to the personal data required(Castaneda & Montoro, 2007).

Furthermore, it is shown that permissions of an app serve the consumer along with ratings as a signal to decide whether an app is trustworthy or not (Bonneau et al., 2009). Permissions contain information about what type of information is accessed by the app. The user has the opportunity to estimate the security and privacy risk, by assessing the sensitivity of the information accessed and by judging the connection between the functions of the app and the permissions needed (Pew Research Center, 2015).One problem in this context is that most users are not able to properly understand and assess the permissions, which is why users often ignore permissions although they seem to not match the functions of the app, which serves as a risk signal (Lin et al., 2012).

The survey of the Pew Research Centre (2015) shows that the permissions required have an influence on user's download intention. In their survey, 60% of the app users indicated that the permissions required to access their personal data are a reason for them to not download an app. In the same survey, 43% of the app users indicated that finding out about permissions granted to an app regarding especially the access to data that is perceived as sensitive are a reason to uninstall an app since they deduce their privacy at risk. Hence, it is shown that permission screens have an important influence on a person's download intention of an app.

Based on the findings of prior research the following hypotheses will be assumed for the study:

**H3: People confronted with highly sensitive permissions a) perceive lower privacy risk b) perceive lower general risk c) have more trust in the app and d) have higher intention to download compared to people confronted with permissions with low sensitivity**

## 2.6. Covariate: Privacy Attitude

Nonetheless, people are very different in their attitude towards their information privacy. According to Westin (1991) there are three different types of people. He describes the privacy fundamentalists to be highly concerned about their privacy. Moreover, he defines pragmatic people whose attitude is filled with medium concerns and finally, he identifies the unconcerned who do not care about their privacy at all. People's privacy attitudes do not need to be regarding to a particular app, it is more a general attitude towards app downloads and the involved risks. According to a survey of Pew Research Center (2014), online users in general indicate that they are highly concerned about their privacy. Prior research showed that people's privacy attitude has an influence on their general need for control, their risk perception and their willingness to take a certain risk (Xu, Dinev, Smith, and Hart, 2011). Based on this, it can be assumed that privacy attitude also has an influence on people's trust in a certain app, their risk perception and their actual download behaviour. This is why privacy attitude is chosen as a covariate for the study at hand. The following hypotheses will be assumed for the influence of privacy attitude:

**H4 People with a higher attitude towards privacy a) perceive higher privacy risk b) perceive higher general risk c) have less trust in the app and d) have lower intention to download an app compared with people with a low attitude towards privacy**

## 2.7. Research Model

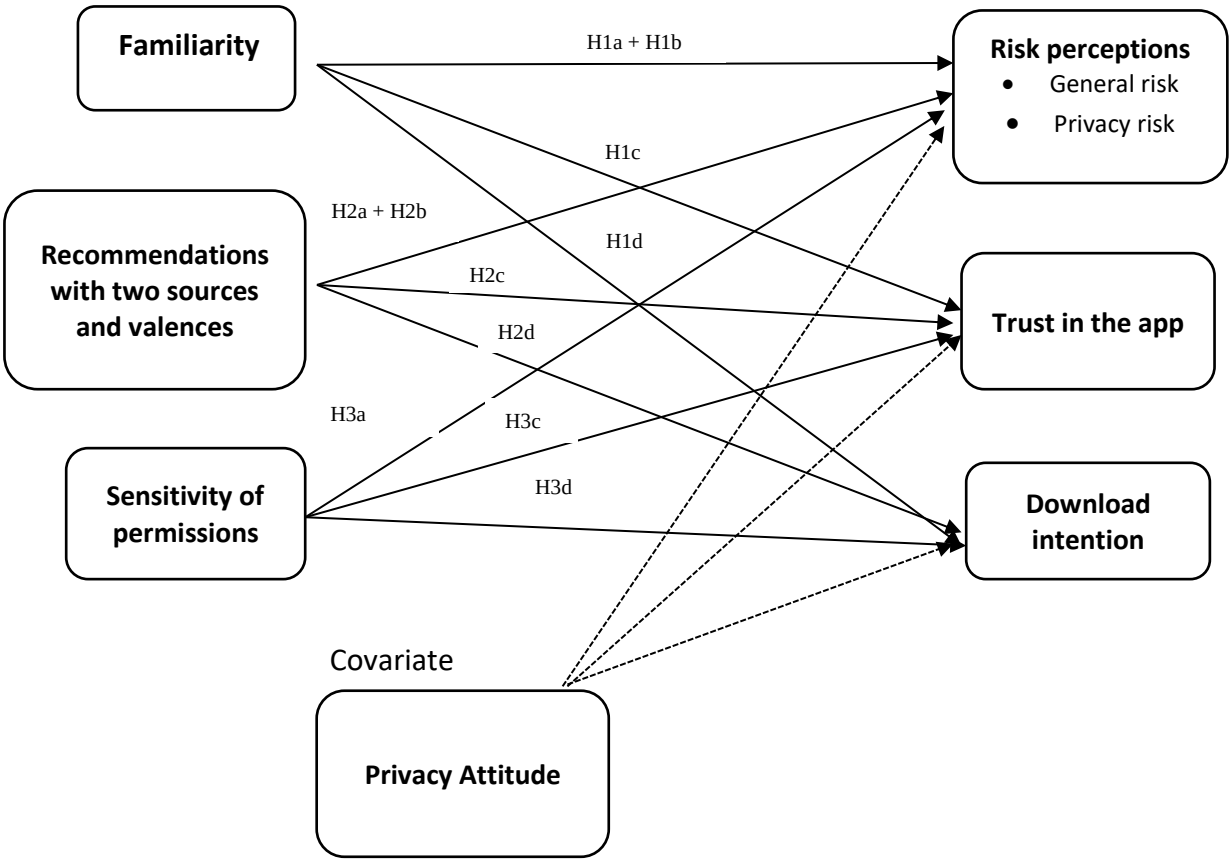



**Figure 1** Research model showing variables and hypotheses

# 3. Methodology

In this method section the research design, the procedure and the participants of the study are going to be described as well as the measurements and manipulations used.

## 3.1. General Design

In this study a 2 (familiar vs unfamiliar) x 2 (friend+/ strangers- vs friend-/ strangers+) x2 (high vs low sensitivity of permissions) experimental study was conducted in order to test the hypotheses and to answer the research questions.

## 3.1. Preliminary study

Before creating the stimulus material for the study two preliminary studies were conducted. The aim of this was firstly to decide on an app appropriate to use for the survey. In order to match the familiarity condition an app was needed that on the one hand people were familiar with but on the other hand they currently did not have on their smartphone. In order to decide on an appropriate app 24 participants were confronted with a list of the 25 most downloaded apps in Germany (Chip, 2016). The results can be found in table 1.For each app they were asked to indicate whether they have heard of the app and whether they currently had that app on their smartphone. It was shown that the app Booking.com had with the highest rates, thus 20 people indicated that they know they app but do not currently have it on their phone.

**Table 1 Preliminary study for choosing an app**

| App | Number of participants who are familiar with this app | Number of Participants who do not currently use the app |
|---|---|---|
| Amazon | 23 | 9 |
| Instagram | 20 | 19 |
| Skype | 21 | 13 |
| Spotify | 22 | 13 |
| Shpock | 12 | 22 |
| Snapchat | 20 | 17 |
| Ebay Kleinanzeigen | 20 | 16 |
| Runtastic | 13 | 17 |
| Wetter.com | 22 | 5 |
| Spielgel | 22 | 16 |
| Bild.de | 19 | 20 |
| DB | 17 | 8 |
| QR code reader | 20 | 6 |
| Angry Birds | 19 | 15 |
| **Booking.com** | **20** | **20** |
| Air B'n'B | 9 | 19 |
| TV Spielfilm | 17 | 15 |
| ZDF | 19 | 15 |
| ARD | 17 | 17 |
| Taschenlampe | 23 | 7 |
| Blitzer.de | 13 | 17 |
| Adblock | 9 | 17 |
| Avira Mobile Security | 15 | 12 |
| Adobe reader | 22 | 4 |
| Radio.de | 11 | 19 |

A second preliminary study was conducted in order to determine the permissions used for the high sensitivity condition and the low sensitivity condition. In order to find out which permissions participants perceive highly sensitive and which less sensitive, they were confronted with a list of the 20 most common permissions used (Pew Research Center, 2015). Participants were then asked to evaluate the sensitivity of the permissions on a 5-point-Likert scale ranging from not sensitive at all (1) to highly sensitive (5). In total, 23 people took part in the survey. The results are shown in table 2. Based on the findings the 5 permissions with the highest means were taken for the high sensitivity condition and the 5 with the lowest mean were taken for the low sensitivity condition. The number of permissions was chosen since the average number of permissions required by an app is 5 (Pew Research Center, 2015).

**Table 2** *Preliminary study for choosing the permissions*

| Permission | Mean | Std. Deviation | Permission | Mean | Std. Deviation |
|---|---|---|---|---|---|
| **Photos/Media/Files: read SD card contents** | **4.36** | **.848** | SMS: Read, send | 3.27 | .767 |
| In-App purchases | 2.29 | 1.231 | Netzworkbased Location | 3.41 | .908 |
| **Search/ find/change personal accounts** | **4.00** | **1.155** | Access to running apps | 3.50 | .859 |
| WLAN- connection information | 3.05 | 1.290 | Full network access | 3.91 | .971 |
| **Read/change personal contact list;** | **4.64** | **.492** | Recall device status and identity | 3.67 | 1.197 |
| Device ID &Call formationen | 3.73 | .935 | **Microphone: record audio** | **3.95** | **1.174** |
| Location (GPS) | 3.82 | 1.097 | Device and app history | 3.14 | .990 |
| Read Google Service configuration | 2.31 | 1.082 | Calender: add/ change appointments | 3.91 | 1.231 |
| **Camera: take photos and record videos** | **4.00** | **1.272** | Control over vibration | 2.23 | 1.066 |
| Informationen about Bluetooth connection | 2.36 | 1.093 | Deactivate sleep mode | 2.24 | 1.053 |

Note. Measured on a five-point-Likert scale; light grey indicates permissions with low sensitivity; bold indicates permissions with high sensitivity

### 3.2. Procedure and stimulus material

Participants of the study were randomly assigned to one of eight fictitious scenarios. This was done with the help of the survey tool “Qualtrics”. Participants were approached via e-mail, Whatsapp and social media.

Before participants were confronted with one of the scenarios, they were asked five questions regarding their demographics, followed by four statements concerning people's attitude towards privacy. Afterwards, a distraction question was inserted in order to prevent that people are focused on the subject of the survey before actually reading the scenarios.

In each scenario people were asked to imagine the download process of an app. In the sequel of this imagined download process they were further confronted with the reviews of the app of strangers and a Whatsapp message of a close friend. Hence, the scenarios are a combination of the familiarity of the app, the valence and source of reviews and the sensitivity of the permissions required.

As mentioned before the participants of the study were asked to imagine the download process of an app. In accordance with the results of the preliminary study, the app Booking.com was chosen for the familiar condition. For the unfamiliar condition a fictitious App was created that resembles Booking.com in order to prevent any bias. For this condition the App Reservation.com was used.

Furthermore, participants were presented with 3 reviews about the app written by strangers. For the reviews, it was controlled for content, this means that the negative reviews contain the exact opposite of the positive reviews. The opinion of a close friend was presented in a Whatsapp message. In order to prevent any influences based on the content, the content of the message contains the same aspects as the reviews, so that it can be ensured that the influence of the source is measured. The aspects dealt with in the reviews and the whatsapp message were for example the operation, design, performance and performance. A star rating was added in order to further highlight the valence of the review. The final design of the reviews can be seen in figures 2.1 and 2.2.


*Figure 2.1 Positive Reviews*


*Figure 2.2. Negative Reviews*

At the end people were presented with the permissions required before actually downloading the app. The permissions were chosen based on the preliminary study that was previously described. The selected permissions for both conditions can be seen in figures 3.1 and 3.2.



*Figure 4.1. Permissions high sensitivity* *Figure 4.2. Permissions low sensitivity*

After seeing one of the scenarios, the participants were confronted with three manipulation check questions, asking participants for their perception of the review, the WhatsApp message and the sensitivity of the permissions. In the next section of the survey people were asked to give their opinion regarding the agreement with statements concerning the trust in the app, their general risk perception, privacy risk perception and download intention.

### 3.3. Pretest

Before the actual study was distributed a pre-test was conducted with 20 participants. The aim of the pre-test was to check whether the scenarios were comprehensible.
Results showed that the different scenarios were interpreted as supposed to.

### 3.4. Participants

Participants for this study were approached via e-mail, Facebook and Whatsapp. In total 315 responses were collected. After cleaning the data set and thus removing all surveys that were incomplete, 285 responses remained. The survey was distributed to German people only. The eight different scenarios were randomly assigned to the participants, which resulted in an average of 35 participants per condition. 115 (40.8%) of the participants were male and 167 (59.2%) were female, three participants refused to indicate their gender. The majority of the participants, 54%, were in the age group 20-29.

Furthermore, most of the participants had higher education (73.2%). Hence, most participants received the highest high school degree possible in Germany (36.8%), 22.8% of the participants had a Bachelor's degree and 11.2% had a Master's degree. This shows that in general the participants of the study were highly educated.

Regarding the smartphone use of participants, the survey showed that the majority of the respondents used Android as operating system (67.4 %) followed by 26.7% of IOS users the remaining 5.9%

indicated that they used Windows as an operating system. Regarding participants' app preferences it was shown that the most used apps were messenger apps (Whatsapp etc.) with 84.9%, Information apps (55.1), social media (40.4%) and apps helping the personal productivity, for example a calendar app (39.6%). An overview of participants' demographics can be found in table 3.

Moreover, a missing value analysis was conducted. This means that missing values regarding the different items were assigned an average in order to avoid any missing values in the further analysis.

**Table 3** Overview of participants' demographics

| | Participants | | | Age Groups | | | | | | | Education | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Scenario | Male | Female | Total | <20 | 20-29 | 30-39 | 40-49 | 50-59 | 60-69 | >70 | No degree | High School (Medium Level) | Apprentice-ship | High School (High Level) | Bachelor's degree or comparable | Master's degree or comparable | Doctorall degree | Other |
| Fam./ Friends+;Stranger-/High Sensivity | 13 | 11 | 24 | 2 | 14 | 1 | 1 | 3 | 2 | 1 | 0 | 1 | 6 | 10 | 4 | 3 | 0 | 0 |
| Unfam./ Friends+;Stranger-/High Sensivity | 9 | 19 | 28 | 1 | 14 | 5 | 2 | 3 | 2 | 1 | 0 | 1 | 6 | 7 | 11 | 3 | 0 | 0 |
| Fam./ Friends+;Stranger-/Low Sensivity | 17 | 19 | 36 | 1 | 20 | 7 | 2 | 6 | 0 | 0 | 0 | 1 | 9 | 11 | 11 | 4 | 0 | 0 |
| Unfam./ Friends+;Strangers-/ Low Sensivity | 19 | 23 | 44 | 2 | 27 | 3 | 3 | 5 | 2 | 1 | 2 | 3 | 10 | 14 | 12 | 2 | 0 | 0 |
| Fam./ Friends-;Strangers+/ High Sensivity | 14 | 26 | 41 | 3 | 22 | 4 | 2 | 10 | 0 | 0 | 0 | 2 | 7 | 17 | 7 | 7 | 0 | 1 |
| Unfam./Friends-;Strangers+/ High Sensivity | 18 | 24 | 42 | 4 | 20 | 2 | 5 | 8 | 1 | 2 | 1 | 1 | 10 | 20 | 3 | 4 | 1 | 2 |
| Fam./ Friends-;Strangers+/ Low Sensivity | 8 | 20 | 28 | 0 | 13 | 6 | 2 | 6 | 1 | 0 | 0 | 0 | 4 | 11 | 8 | 3 | 0 | 2 |
| Unfam./Friends-;Strangers+/ Low Sensivity | 17 | 23 | 40 | 5 | 24 | 6 | 2 | 3 | 0 | 0 | 1 | 2 | 7 | 15 | 9 | 6 | 0 | 0 |

### 3.5. Measurements

After the data for the survey had been collected a factor analysis was conducted in order to identify the components of the covariate and the dependent variables. Therefore, an orthogonal rotation (Varimax) was conducted for 26 items. The KMO (Kaiser-Meyer Olkin) showed that the sample is factorable (.90). The result showed that the items are categorized into 6 dimensions, which means that there is one extra dimension measured (Table 4). In the following the individual constructs and their reliability will be further explained.

**Table 4 Factor analysis**

| Constructs | Components | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **Privacy Risk** | | | | | | |
| 1. I am concerned that information collected about me by the app could be misused | | | .844 | | | |
| 2. I would be concerned about privacy of personal information the app collects about me | | | .804 | | | |
| 3. I would be concerned that personal information about me collected from the app could be used in a ways I did not foresee | | | .826 | | | |
| **General Risk** | | | | | | |
| 1. Downloading this app involves more risk than downloading other apps | | | | | .717 | |
| 2. The decision to install this app is risky | | | | | .753 | |
| 3. I believe installing this app is harmful | | | | | .785 | |
| 4. Downloading this app could involve important financial losses | | | | | .574 | |
| 5. As I consider downloading this app, I worry whether the app will perfom as it's supposed to | | | | | | .828 |
| 6. As I consider downloading this app, I am concerned about the reliability | | | | | | .882 |
| 7. I have confidence in the security when downloading this mobile application | | | .554 | | | |
| 8. I am confident that my personal information will not be exposed to inappropriate parties | | | .572 | | | |
| **Trust** | | | | | | |
| 1. This app is trustworthy | | .532 | | | - .455 | |
| 2. This app has my bests interests in mind | | .686 | | | | |

**Table 4 continued**

| | | | | | | |
|---|---|---|---|---|---|---|
| 3. This app has high integrity | | .823 | | | | |
| 4. I trust this app to make an effort to keep my personal information out of the hands of unauthorized individuals | | .749 | | | | |
| 5. I trust this app/mobile apps not release personal information about me without my express permission | | .706 | | | | |
| 6. I trust the app to function as it is supposed to | | .462 | | | | -.570 |
| **Download Intention** | | | | | | |
| 1. I will not hesitate downloading this app | .659 | | | | | |
| 2. The probability that I will download this app is high | .849 | | | | | |
| 3. I am most likely to download this app | .894 | | | | | |
| 4. I intend to use this app | .855 | | | | | |
| **Privacy Attitude** | | | | | | |
| 1. For me it is most important that my information remains private | | | | .860 | | |
| 2. Compared to others I am more concerned about potential dangers that threaten my privacy | | | | .743 | | |
| 3. I think it is important that I have control over who can access my personal information | | | | .875 | | |
| 4. I am convinced that my privacy should be respected and protected | | | | .730 | | |

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 6 iterations.

Note. Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 6 iterations.

The covariate in this study is privacy attitude. It consists of four items adapted from Xu et al.( 2011) and Beldad (2015). A five-point Linkert scale was used for all the items ranging from (1) strongly disagree to (5) strongly agree. The reliability check showed that with a Cronbach's alpha of .83 the construct is reliable.

There were four dependent variables in this study which include privacy risk, general risk, trust and download intention. All these variables were measured on a five-point Likert scale ranging from (1) strongly disagree to (5) strongly agree. The items for privacy risk were adapted from Tayler et al. (2009). The privacy risk construct originally consisted of three items. The factor analysis showed that two of the risk items measure the same dimension. This is why the two items 'I am concerned that through the download of this app unauthorised parties will have access to my personal data' and 'I am concerned that my personal data will be passed on to third parties' are added to the privacy concerns construct. With a Cronbach's alpha of .92 this construct was found to be reliable.

Risk was originally measured by eight items that were adapted from Harris et al. (2016), Stone and Gronhaug (1993) and Pavlou and Chellapalla (2013). As previously mentioned two risk items were added to privacy concerns. In addition to this, the factor analysis showed that the risk items measure an extra dimension. Based on this the risk items 'Regarding the download of this app, I am concerned that it does not work as it is supposed to' and 'Regarding the download of this app, I am concerned whether this app will work without errors' will form a new construct called technical risk which is shown to be reliable with a Cronbach's alpha of .83. The general risk construct consists of four remaining items, the reliability check resulted in a Cronbach's alpha of .86.

The next dependent variable used in this study was trust, which was originally measured with six items. The factor analysis showed that among these items there are two ambiguous items which are 'This app seems trustworthy' and 'I have trust that this app fulfils its functions'. These two items were removed from the construct. The remaining items were found to be reliable with a Cronbach's alpha of .87. Two of these items were adopted from Taylor et al. (2009), one was adopted from Harris et al. (2016) and one item was self-formulated.

The last variable of the study is download intention, which consists of four items adopted from Taylor et al. (2009) and one item adapted from Maxham and Netemeyer (2002). The reliability check resulted in a Cronbach's alpha .91, which shows a high reliability. An overview of all reliabilities can be found in table 5.

**Table 5** Reliabilities of the constructs

| Construct | Items | Cronbach's alpha | Mean | STD |
|---|---|---|---|---|
| Privacy Attitude | 4 | .83 | 4.15 | 1.06 |
| Privacy Risk | 5 | .91 | 3.91 | 1.09 |
| General Risk | 4 | .81 | 3.00 | 1.26 |
| Technical Risk | 2 | .84 | 3.34 | 1.21 |
| Trust | 4 | .87 | 2.18 | .94 |

Note. Measured on a five-point Likert scale

### 3.6. Manipulation Check Main Study

After the reliability of the individual constructs was checked, a manipulation check was conducted in order to determine whether participants correctly understood the manipulated stimulus material. For the manipulation of the independent variable familiarity a screening question was added to the survey.

This means that participants in the familiar condition were asked whether they know the App Booking.com and whether they currently have the App on their smartphone. Participants who either did not know the App or already had the app on their phone were directly lead to the end of the survey. This way it was made sure that only people who fulfil the criteria for the familiarity condition could take part in the survey. Participants who were assigned to the unfamiliar condition were asked if they know the fictitious App Reservation.com as a control question. It was shown that all the participants in this condition noticed that is an unfamiliar App.

There were three control questions used in the survey. Two were asking people to indicate their perception of the valence of the review and the message of a close friend on a five-point Likert scale ranging from (1) negative to (5) positive. In the third one participants were asked to indicate how sensitive they would rate the permissions required on a scale from (1) not sensitive at all to (5) extremely sensitive.

The Manipulation Check was conducted with the help of a t-test. A significant difference was shown for the manipulation of the reviews. Results show that for the positive condition it was shown that participants rated reviews significantly higher ($M=3.67$, $SD=1.29$) in the positive condition compared to the negative condition ($M=1.69$, $SD=.96$) with $t= 14.56$ and $p<.001$. Participants who were confronted with a negative message of a close friend rated the message significantly more negative ($M=1.85$, $SD=1.38$) compared to the positive condition ($M=3.97$, $SD=1.05$) with $t=14.40$ and $p<.001$.

The manipulation check also showed that also the manipulations for sensitivity were significant. It was shown that participants confronted with the low sensitivity condition were rated significantly lower ($M=2.3$, $SD=1.35$) than the people confronted with the high sensitivity condition ($M=3.5$, $SD=1.5$) with $t=3.7$ and $p<.001$.

## 4.Results

In this section the main results of this study will be discussed. These include main effects as well as interaction effects. The independent variables in this study are as mentioned before the familiarity of the app, reviews with different source and valence and the sensitivity of the permissions required for downloading the app. Covariate in this context is privacy attitude**.**

### 4.1. Correlation analysis

Before the MANOVA and MANCOVA a correlation analysis was conducted. The results suggest imply that four out of five correlations were significant. The correlation for privacy risk is significant at the .05 (two-tailed) level (r (.444), p<.001). Also, statistical significance was found for general risk perception (r (.234), p<.001) and technical risk perception (r (.176), p=.003). Furthermore, the correlation for download intention was found to be significant (r (-.128) p=.032). These correlations form one of the basic assumptions in order to proceed with with MANOVA and MANCOVA.

### 4.2. MANOVA and MANCOVA

A Multivariate Analysis of Variance (MANOVA) and a Multivariate Analysis of Covariance (MANCOVA) were conducted by means of SPSS in order to test the hypotheses. The MANOVA allows to compare multivariate sample means. Hence, it helps to identify the influence of changes in the independent variables on the dependent variables. Furthermore, the analysis allows to identify the relationships among the dependent variables as well as the independent variables. In addition to this, the MANCOVA analyses the influence of a covariate in this case privacy attitude. In the following the results of the MANOVA are discussed and compared to the results of the MANCOVA. An overview of the results can be found in table 3 and 4.

Before conducting the MANOVA and MANCOVA, the assumptions were tested. No severe violations of the assumptions were found.

**Table 3** Descriptive statistics of the Main effects

| | **Mean (SD)** | | | | |
|---|---|---|---|---|---|
| | Privacy Risk [a] | General Risk [a] | Technical Risk [a] | Download Intention[a] | Trust[2] |
| Familiar | 3.89 (.91) | 2.97(.88) | **3.22 (1.08)** | 1.71 (.89) | 2.24 (.87) |
| Unfamiliar | 3.92 (.87) | 2.99 (.92) | **3.45(.96)** | 1.65 (.69) | 2.12 (.87) |
| Friends+/Strangers- | 3.86 (.84) | 2.92 (.82) | 3.30 (.97) | 1.66 (.78) | 2.19 (.80) |
| Friends-/Strangers+ | 3.94 (.94) | 3.05 (.96) | 3.38 (1.06) | 1.69 (.81) | 2.16 (.85) |
| High Sensitivity | **4.08 (.88)** | **3.13 (.95)** | 3.29 (1.06) | 1.64 (.79) | 2.12 (.83) |
| Low Sensitivity | **3.75 (.88)** | **2.85 (.83)** | 3.39 (.99) | 1.71 (.79) | 2.23 (.81) |

*Notes.* Measured on a 5-point Likert-scale (1=strongly disagree, 5= strongly agree)

**Table 4** Multivariate Analysis of Covariance

| | F (p) | | | | | | |
|---|---|---|---|---|---|---|---|
| | Privacy Risk | General Risk | Technical Risk | Download Intention | Trust | Pillai's Trace | $\eta^2$ |
| Privacy attitude | **75.402 (.000)** | **16.782 (.000)** | **10.353 (.001)** | **4.605 (.033)** | **3.404 (.066)** | **17.578 (.000)** | .246 |
| Source/Valence | .663 (.416) | 1.067 (.303) | 1.289 (.257) | .217 (.642) | .033 (.856) | .618 (.686) | .011 |
| Sensitivity | **11.709 (.001)** | **6.556 (.001)** | 1.017 (.341) | .761 (.384) | 1.384 (.240) | **3.966 (.002)** | .069 |
| Familiarity | 1.604 (.206) | .737 (.391) | **5.229 (.023)** | .753 (.386) | 2.428 (.120) | 1.196 (.312) | .022 |
| Source/Valence* Sensitivity | 1.113 (.292) | .128 (.721) | .195 (.659) | .153 (.696) | .275 (.601) | .790 (.557) | .014 |
| Source/Valence* Familiarity | .342 (.559) | .005 (.941) | .834 (.362) | .159 (.691) | .369 (.544) | .676 (.642) | .012 |
| Sensitivity* Familiarity | 1.067 (.303) | 1.033 (.310) | .735 (.392) | .003 (.957) | .169 (.682) | 1.241 (.290) | .023 |
| Source/Valence* Familiarity* Sensitivity | .024 (.878) | .174 (.677) | .280 (.597) | .002 (.962) | .258 (.612) | .203 (.961) | .004 |

*Notes.* Values in bold are significant at p< .05

### *Familiarity*

Regarding the familiarity of the App the Wilk's Lambda indicated that familiarity has no main effect on the dependent variables (F=1.06, p=.385). However the Test of Between-Subjects Effects showed that there is a significant main effect to be found for the perception of technical risk (F=5.229, p=.023). Hence, it is shown that participants confronted with a familiar app perceive the technical risk to be lower (M=3.2, SD=.092) compared to participants confronted with an unfamiliar app (M=3.45, SD=.083). Hence, H2e is supported. In contrast to this there was no evidence found for H2a, H2b, H2c and H2d. Hence, there was no significant main effect found for familiarity on privacy risk (F=.10, p=.747), on the general risk perception (F=.16, p=.692) and on download intention (F=.411, p=.522). Although there was a slight difference for trust between the familiar app (M=2.24, SD=.07) and the unfamiliar app (M=2.11, SD=.07), this difference was not significant. Although there was a slight difference for trust between the familiar app (M=2.24, SD=.07) and the unfamiliar app (M=2.11, SD=.07), this difference was not significant.

### *Source and Valence of Reviews*

There was no significant main effect found for the Reviews with different source and valence. No evidence was found for H3a, H3b, H3c, and H3d. The reviews with different source and valence had no significant effect on privacy risk (F=.06, p=.802), general risk perception (F=.60, p=.440) and technical risk (F=.86, p=.348). It was shown that there was no significant difference between the download

intention between the two conditions (F=.35, p=.555). Also, there was no difference found for the trust in the app (F=.01, p=.932). Also, there was no difference found for the trust in the app (F=.01, p=.932).

## Sensitivity

The Wilk's Lambda score showed that there is a significant main effect of sensitivity on the dependent variables (F=3.96, p=.002). The Between-Subjects Effect Tests yielded more information about this main effect. It was shown that participants confronted with less sensitive permissions required for the download of the app perceive lower privacy risk (M=3.75, SD=.07) than people confronted with permissions with high sensitivity (M=4.08, SD=.88) this difference was found to be significant (F=11.709, p=.001) this showed that H1a is supported. Furthermore, there was a difference in the means for general risk perception between permissions with high sensitivity (M=3.13, SD=.95) and permissions with low sensitivity (M=2.85, SD=.083), this difference is significant (F=6.56, p=.001) thus H1b is supported. There was a slight difference in the means for technical risk between the high sensitivity condition (M=3.39, SD=.085) and the low sensitivity condition (M=3.27, SD=.09), but this difference was not significant (F=1.02, p=.313). Hence, H1e is not confirmed. Also, there was no evidence found for the influence of sensitivity on download intention (F=.75, p=.388) and trust (F=1.34, p=.248).

### Interaction effects

There was no interaction effect found for Familiarity*Sensitivity (F=1.24, p=.29). No evidence was found for an interaction between Familiarity and Source/Valence (F=.68, p=.642). Also, there was also no interaction effect for Source/ Valence and Sensitivity (F=.79, p=.557). Eventually, no three-way interaction was found for the three independent variables (F=.203,p=.961).

## MANCOVA

After the MANOVA a MANCOVA was conducted in order to see the differences in the two analyses and to determine the influence of the covariate. It was shown that there were no differences regarding the main and interaction effects. Although means were slightly higher in the MANCOVA, there were no changes regarding the significances of effects. Furthermore, the MANCOVA yielded that there is a significant main effect of the covariate privacy attitude. Pillai's trace indicated the significant effect of the covariate on all the dependent variables with F=17.58 and p<.001.

### Main effects of the covariate: Privacy attitude

The Test of Between-Subjects Effects indicated that privacy attitude had a significant influence on privacy risk (F= 75.40, p<.001. Hence, people who have a high score for privacy attitude also perceive high privacy risk concerning the download of the app. The effect of privacy attitude on general risk perception was significant as well (F=16.78, p<.001). Furthermore, a significant influence was shown for the relationship between privacy attitude and technical risk (F=10.35, p=.001). Privacy attitude has a significant influence on download intention (F=4.61, p=.003). Moreover, a marginally significant effect was found for privacy attitude on trust (F=3.40, p=.066).

### 4.1. Summary of the hypotheses

The following figure shows an overview of the hypotheses and whether they were supported or not

| | Hypothesis | Result |
|---|---|---|
| **H1a** | People confronted with a familiar app perceive lower privacy risk than people confronted with an unfamiliar app | **Not supported** |
| **H1b** | People confronted with a familiar app perceive lower general risk than people confronted with an unfamiliar app | **Not supported** |
| **H1c** | People confronted with a familiar app have higher trust in the app than people confronted with an unfamiliar app | **Not supported** |
| **H1d** | People confronted with a familiar app have higher intention to download than people confronted with an unfamiliar app | **Not supported** |
| **H2a** | People confronted with a positive recommendation of a close friend and negative recommendations of strangers perceive lower privacy risk than people confronted with the a negative recommendation of a close friend and positive recommendations of strangers | **Not supported** |
| **H2b** | People confronted with a positive recommendation of a close friend and negative recommendations of strangers perceive lower general risk than people confronted with the a negative recommendation of a close friend and positive recommendations of strangers | **Not supported** |
| **H2c** | People confronted with a positive recommendation of a close friend and negative recommendations of strangers have higher trust in the app than people confronted with the a negative recommendation of a close friend and positive recommendations of strangers | **Not supported** |
| **H2d** | People confronted with a positive recommendation of a close friend and negative recommendations of strangers have higher intention to download than people confronted with the a negative recommendation of a close friend and positive recommendations of strangers | **Not supported** |
| **H3a** | People confronted with highly sensitive permissions perceive higher privacy risk than people confronted with little sensitive permissions | **Supported** |
| **H3b** | People confronted with highly sensitive permissions perceive the general risk to be higher than people confronted with little sensitive permissions | **Supported** |
| **H3c** | People confronted with highly sensitive permissions have lower trust in the app compared to people confronted with little sensitive permissions | **Not supported** |
| **H3d** | People confronted with highly sensitive permissions have lower intention to download compared to people confronted with little sensitive permissions | **Not supported** |
| **H4a** | People with a higher attitude towards privacy perceive higher privacy risk compared to people with a low attitude towards privacy | **Supported** |
| **H4b** | People with a higher attitude towards privacy perceive higher general risk to download compared to people with a low attitude towards privacy | **Supported** |
| **H4c** | People with a higher attitude towards privacy have lower trust in the app compared to people with a low attitude towards privacy | **Supported** |
| **H4d** | People with a high attitude towards privacy have lower intention to download Compared to people with a low attitude towards privacy | **Supported** |

## 5. Discussion

The purpose of the study at hand was to examine the influence of familiarity, sensitivity of permissions required and reviews with different source and valence on people's risk perception and their willingness to download an app. Therefore, a 2x2x2 experiment was conducted. In the following the key findings of this study, the theoretical and practical implications, as well as limitations and suggestions for future research will be discussed

### 5.1. Key Findings

The study at hand examines whether familiarity, recommendations with different source and valence and the sensitivity of permissions have an effect on risk perception and download intention. In the following, the main findings will be discussed per independent variable and connected to the findings of prior research in the field.

**Main effect of familiarity**

It was hypothesised that the familiarity with an app positively influences people's risk perception and their willingness to download the app. These assumptions were not entirely confirmed. Results showed only one significant main effect for familiarity. Hence, it was found that if confronted with a familiar app potential users perceive the technical risk to be lower. This means that people have less concerns about the proper functioning of the app if they know the app. This partly confirms the findings Gefen (2000), who pointed out that familiarity helps to reduce uncertainties towards a new app and that familiarity reduces the complexity of a decision process. However, results showed that only technical risk was found to be significantly influenced by familiarity. There were no significant main effects found for privacy risk and general risk perception. The reason for this might be a general attitude towards making purchases via an app. The research of Chen et al. ( 2016) points out that about 60% of the smartphone users are highly concerned about purchasing items via an app since they see their personal data at risk. Moreover, the research points out that people do not feel safe regarding making purchases via an app or having to share for example their credit card details. The app dealt with in the study at hand is an app that people can use to book their journeys which can be related to higher costs, since travelling is mostly expensive. It can thus be assumed that since the booking of for example flights or hotels is assumed with expenses, and thus associated with higher risk in general, people's intention to download this type of app might generally be lower. Furthermore, it can be assumed that familiarity in this context does not outbalance these risk perceptions.

Moreover, there was no significant influence found of familiarity on download intention. This finding is in line with the research of Chen et al. (2016) who examined the effect of familiarity on app adoption. Their research states that there is no effect of familiarity on the intention to install an app. A reason for this might be there are other influences that have a stronger influence on the intention to download an app. Rogers (1995) suggests for example that the benefits offered need to be taken into accout with regards to the adoption of a new technology.

Another reason why familiarity might only have little influence on download intention, is that the general importance of familiarity with regards to apps is low. The research of Brookshire et al.(2016) showed that familiarity is less important for the download behaviour of apps. It was shown in their research that people's willingness to download an app was not related to the familiarity of the app. The consumer behaviour research of Localitics (2016) adds that when searching an app, people focus searching for a type of app or the ranking in the app store instead of looking for specific apps. This shows that there might be different criteria for people why and how they search and choose an app. In this process familiarity seems to not have a high influence.

**Main effect of recommendations with different source and valence**

The aim of the study at hand was to examine the influence of recommendations if users are confronted with two different sources stating contradictory opinions about the app. It was assumed that users are more influenced by the recommendations of a close friend.

This hypothesis was not confirmed. It was shown that the recommendations with different source and valence do not have a significant influence on people's risk perception and their willingness to download the app. Research on the one hand suggests that the opinion of important others are an important influence regarding people's willingness to use a new technology(Kijsanayotin et al., 2009).

On the other hand there is also research that found evidence for the influence of reviews by strangers. Although prior research suggests that a strong tie strength which is present for friends increases the importance of an opinion to the user (Lee et al., 2009) the results of the study at hand do not confirm this. It was shown that there was no dominant source for people in the study. One reason for this might be that the two different sources of reviews evoked the same perception of importance. Hence, people might not perceive the opinion of a close friend more important than the reviews written by strangers. In addition to this it might be explained by the setup of the study. People were confronted with two reviews, firstly the reviews by strangers that can be seen before actually downloading an app afterwards the participants were confronted with opinion of a close friend that was contradictory to the valence of the reviews. Hence, in the sequel of the study people were confronted with both a positive and a negative opinion. A possible explanation for the fact that there was no effect found is that the opinions balance each other out and that therefore there was no source to be found as having a dominant influence. Also, the fact that the results are not in line with prior studies might be explained by a lack of interest in the type of app. Hence, participants in real life might not have interest in downloading a travel app and therefore they still did not have the intention to download that type of app after reading the reviews.

**Main effect of sensitivity**

This study examined the effects of the sensitivity of the permissions that an app requires on people's risk perception and their download intention. It was hypothesized that permissions with high sensitivity lead to higher risk perception and lower download intention compared to permissions with low sensitivity. The hypotheses were partly supported by the study at hand.

Results showed that there is a main effect for sensitivity on privacy risk.It was shown that people who were confronted with highly sensitive permissions required had higher concerns about their privacy. These findings are in line with the research of Agarwal, Kim and Malhotra (2004) who found that the sensitivity of the information required leads to a higher perception of the risk. Hence, the more sensitive data is required by an app the more people see the protection of their own privacy at risk.

If the privacy risk is perceived as being very high this also negatively influences people's willingness to allow the access to private data (Castaneda & Montoro, 2007). A reason for this might be that people perceive the permissions as too sensitive. Since the download of mobile apps involves a lack of control regarding the handling of personal data, requiring access to highly sensitive data can be seen as critical factor leading to higher privacy risk perception (Pan& Zinkhan, 2006).

In the context of an app download rejecting the access to personal data automatically means that the app cannot be downloaded. This shows that it is of special importance to ensure people safety about the handling of the personal data accessed in order to create a feeling of trust and redeem privacy concerns.

Also, a significant main effect was found for general risk perception. This shows that the sensitivity of the permissions required do not only make people feel more concerned about their privacy, but they also evaluate the download of the app as more risky in general. This means that by requiring access to data that is perceived as highly sensitive, people also see for example higher technical risk or performance risk. Hence, it is shown that app permission can have a negative influence on people's general attitude towards the app, which means that the formation of a positive attitude towards the app that is necessary for the decision to download the app is hindered (Kim, Ferrin, & Rao, 2008).

Surprisingly, there was no main effect found for the sensitivity of the permissions required on the intention to download the app. This is contradictory to prior research (Castaneda & Montoro, 2007). An explanation for this might be that there are underlying factors involved in the decision to download an app that were not involved in this research. Hence, the need for further research is highlighted. The mean score for download intention was generally low in the survey (M=1.67,SD=.73). A reason for this might be as previously mentioned that there was no interest in the type of app used in the study among participants which means that in general the intention to download a booking app was rather low.

**Main effect of privacy attitude**

The most influential factor found in the study at hand is people's privacy attitude. There were significant main effects found for privacy attitude on all the dependent variables. Privacy attitude served as a covariate in the study at hand. It measured people's general attitude towards privacy prior to any influence. It was shown that in general people in this study had a high score for privacy attitude (M=4.14, SD=.83) measured on a 5-point-Likert-Scale. Prior research showed that people's privacy attitude has an influence on their general need for control, their risk perception and their willingness to take a certain risk (Xu, Dinev, Smith, and Hart,2011). This was also confirmed by this study. Furthermore, the high score for privacy attitude also serves as a potential explanation for the little main effects found for familiarity. A high score on privacy attitude indicates that in general participants were sceptical regarding privacy protection of apps and the general risk involved at the same time having a high need for privacy security. This shows the sceptical attitude of participants before starting the survey and before being confronted with the manipulation material. Hence, the attitude of the participants was a dominant factor that could not be outbalanced for example by people's familiarity with an app. Furthermore, people who have a high valuation of their privacy, have higher risk perception regarding the privacy risk or general risk involved in the download of an app. According to Xu et al. (2011) higher concerns about privacy protection lead to less willingness to provide access to personal information, which is a condition for the download of an app.

## 5.2. Theoretical and managerial implications

Two kinds of implications can be derived from the current study, theoretical and managerial implications. First the theoretical implications are going to be discussed followed by the managerial implications.

The aim of this study was to give an insight in people's download behaviour regarding mobile apps and the influencing factors on their risk perceptions.

First of all, important knowledge was gained regarding the influence of familiarity in the context of app downloads. It was shown that while for online shopping research claims familiarity to be one of the most influential factors, it is less important in the context of mobile apps. It was shown to not have an influence on users' privacy risk and general risk perception. It shows that familiarity does not help to reduce people's privacy concerns. Hence, the difference in perception towards e-commerce is shown. This means that familiarity is not enough to reduce people's privacy concerns, it only helps to reduce people's technical risk. Thus, users have more trust in the proper functioning of the app if they are familiar with it. However, familiarity is not influential enough to reduce people's concerns about their privacy and risk in general.

Moreover, it was shown that permissions have a high influence on people's perception. Hence, people see their privacy more at risk if they perceive the access of information required as highly sensitive. App permissions are part of every download process, this means that there is no possibility to change the permissions or make them less sensitive. This highlights the fact, that it is very important to further investigate how people's perception of privacy risk and general risk can be lowered. At least, it needs to be examined how people perceive the privacy risk and general risk as less prominent in the download process of an app.

Furthermore, it was found that the German participants of the study had a high attitude towards privacy. This implies that they are very sceptical regarding the safety of their private information. Their general attitude towards privacy was shown to have a high influence on their risk perception and their download intention. It was shown that positive reviews of close friends or reviews in general were not able to outbalance their sceptical attitude and neither was the familiarity with the app. This leads to the necessity to investigate the underlying mechanisms to reduce their general scepticism towards apps to ensure that there are less perceived risks involved in the download process.

In addition to the theoretical implications, there are also managerial implications that can be derived from this study.

Firstly, it was shown that familiarity is not an influential factor to reduce privacy risk and general risk, neither for increasing their download intention. This shows that managers need to understand the ways that people use to find an app and how they decide to download it. The analytics company Loyalitics (2015) for example points out that app users do not explicitly search for an app name, users are focused on certain app types that they look for or they discover a new app by its ranking in the app store. This highlights the fact that instead of increasing their brand awareness, marketers for apps should focus on their ranking in the Google Play store and their findability.

Furthermore, it was shown that permissions have a rather negative influence on people's risk perception regarding privacy risk and general risk. In addition to this, it was shown that the German participants of the study highly valued their privacy. Hence, it is shown that it is of major importance to provide people with a secure feeling about the download of an app and this way to generally address their sceptical attitude.

One possible way to achieve this might be to highlight the value of the app to the consumer. This way the consumer might be more focused on the benefits that might outweigh the risks. According to the privacy calculus this can positively influence their users in their decision making process.

It is shown that marketers in general need to highlight the safety of the download and ensure users that their personal data is handled right and not for example passed on to third parties. In order to achieve this, an independent seal might help to ensure the safety of an app. In Germany there is for example the "Trusted App" seal (App Security Center, 2016), this seal certifies that private information is handled properly by the app and that the download is safe. This might be one way to address people's scepticism and to reduce their perceived privacy risk and general risk.

Furthermore, security indicators could directly be involved in the search process. This means when people are looking for an app in the app store the list of results could directly contain positive indicators about the security of the app. This way, users directly obtain the information needed to reduce their concerns.

### 5.3. Limitations and Future Research

The results of this study have to be regarded with some limitations. Firstly, only German participants were included in the study, this means that there might have been a cultural influence on the results.

According to the cultural typology of Hofstede (2001) Germany has a high score on the dimension of uncertainty avoidance. This dimension describes the extent to which members of a culture feel threatened by unknown situations and try to avoid these (Hofstede, 2001). The high score of Germany on this dimension implies that Germans have a tendency to avoid uncertainties. The download of a mobile app includes various uncertainties especially about the handling with personal data and potential negative consequences (Featherman & Pavlou, 2003; Featherman & Wells, 2004). The high uncertainty avoidance of the German participants might also have an influence on the results and the low scores on download intention in general ($M=1.67, SD=.73$). This means that for future research it would be interesting to include different cultures in the participants.

Furthermore, there was no equal distribution in this study. This means that the individual scenarios were not seen by an equal number of participants. This may also have an influence on the results and their generalizability. For future research it would be advisable to pay attention to an equal distribution in order to avoid this.

Moreover, there might be limitations to the research model. In this study the influence of recommendations with different source and valence were tested. Both sources were combined in one scenario with contradictory opinions about the app. It was shown that there was no effect. For future research it could be interesting to handle the different sources in different scenarios, this way it can be prevented that the contradictory opinions balance each other out.

For future research, it might also be interesting to include the interest in the app type dealt with in the scenarios. In this study it was dealt with a booking app, but the interest of people in this type of app was not taken into account in the research. Hence, this would be recommendable for future research.

Finally, future research should focus on investigating the influence of other potential factors on people's download intention and their risk perception in order to identify the underlying factors in the decision-making process of mobile apps.

### 5.4. Conclusion

The influence of mobile apps is steadily growing, this is why it is important to understand how the privacy risk and the general risk perception can be reduced. This study investigated the influence of

familiarity, recommendations with different source and valence and the sensitivity of the permissions required.

It was shown that familiarity only had little influence on users. It only helped to reduce their technical risk perception, which shows that people have more trust in the proper functioning of the app, if it is familiar. Furthermore, there was no effect found of familiarity on privacy risk perception, general risk perception or on download intention.

It was shown that the sensitivity of the permissions required by the app had an effect on people's perception of the privacy risk involved and their general risk perception. Surprisingly, there was no effect found for the sensitivity of the permissions on people's download intention, which highlights the need for further research to identify the underlying mechanisms for the download of mobile apps. The most influential factor in this study having an effect on risk perception concerning privacy risk, technical risk and general risk and people's intention to download, is the attitude towards privacy. It was shown that among the participants, the majority had a high valuation of their private information which resulted in more scepticism towards the download of apps in general. Because of this attitude, it is essential to provide users with a feeling of safety during the download process and provide them with indicators that proof the safety of the app.

## 6. References

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

Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human Decision Processes, 50 (2), 179-211.

Antón, A.I., Bertino, E., Li, N.,& Yu, T. (2007). A roadmap for comprehensive online privacy policy management, Commun. ACM 50 (7), 109-116.

Antón, A.I., Earp, J.B., He, Q., Shufflebeam, W., Bolchini, D., & Jensen, C. (2004). The Lack of clarity in financial privacy policies and the need for standardization. IEEE Security and Privacy (2:2), 36-45.

Arndt, J. (1967). Role of product-related conversations in the diffusion of a new product. Journal of Marketing Research, 4 (3), 291-295.

Bagozzi, R.P.,& Dholakia, U.M. (2002). Intentional social action in virtual communities. Journal of Interactive Marketing, 16 (2), 2-21.

Bagozzi, R.P.,& Lee, K.H. (2002). Multiple routes for social influence: the role of compliance, internalization, and social identity. Social Psychology Quarterly, 65 (3), 226-247.

Bansal, H.S., &Voyer, P.A. (2000). Word-of-mouth processes within a services purchase decision context. Journal of Service Research, 3 (2), 166-177.

Baumer, D.L., Earp, J.B.,& Poindexter, J.C. (2004). Internet privacy law: A comparison between the United States and the European Union. Computers & Security, 23 (5), 400-412.

Benjamin, F. (2015). Mobile App Report. Accessed on 21/05/2016. Retrieved from: https://www.linkedin.com/pulse/how-do-people-discover-mobile-apps-what-influences-freddie-benjamin.

Bonneau, J., Anderson, J., & Church, L. (2009). Privacy suites: shared privacy for social networks. In Proc. of the 5th Symposium on Usable Privacy and Security, SOUPS ’09.

Brown, J., Brodering, A., & Lee, N. (2007). Word of mouth communication within online communities: Conceptualizing the online social network. Journal of interactive marketing, 21 (3), 2-20.

Business of Apps, (2015). App Usage Statistics. Accessed on 22/05/2016. Retrieved from: http://www.businessofapps.com//app-usage-statistics-2015/.

Canfora, G., Constante, E., Pennino, I.,&Visaggio, C.A. (2008). A three-layered model to implement data privacy policies, Comput. Stand Interfaces 26 (6), 398-409.

Castañeda, J. A., & Montoro, F. J. (2007). The effect of Internet general privacy concern on customer behavior. Electronic Commerce Research, 7(2), 117-141.

Chang, M., & Wu, W. (2012). Revisiting perceived risk in the context of online shopping: an alternative perspective of decision-making styles. Psychology & Marketing, 29(5), 378–400.

Chevalier, J. A., &Mayzlin, D. (2006). The effect of word of mouth on sales: Online book reviews. Journal of marketing research, 43(3), 345-354.

Cheung, C.M.K., Chiu, P.-Y.,& Lee, M.K.O. (2011). Online social networks: why do students use Facebook? Computers in Human Behavior, 27 (4), 1337-1343.

Cheung, C.M.K.,& Lee, M.K.O. (2010). A theoretical model of intentional social action in online social networks, Decision Support Systems, 49 (1), 24-30.

Chip (2016). Download Charts der Woche. Accessed on 20/07/2016 from http://www.chip.de/Handy-Downloads-Download-Charts-Top-100-der-Woche_50159909.html?xbl_category=60988

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

Culnan, M. J. (1993). " How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. MIS quarterly, 341-363.
ISO 690

Currie, R.R., Wesley, F., & Sutherland, P. (2008). Going where the Joneses go: Understanding how others influence travel decision-making, International Journal of Culture, Tourism Hosp. Res. 2, 12-24.

Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13 (3), 319-340.

Dembski, W.A. (1998). The Design Inference. Cambridge Univerity Press, Cambridge, United Kingdom.
Dhillon, G.,& Backhouse, J. (1996) Risks in the use of information technology within organizations. International Journal of Information Management 16 (1), 65-74.

DiPietro, R. B., Wang, Y., Rompf, P. and Severt, D. (2007), At-destination visitor information search and venue decision strategies. Int. J. Tourism Res., 9, 175–188.

Dowling, G. R., &Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. Journal of consumer research, 21(1), 119-134.

Ermakova, T., Baumann, A.,Fabian, B.,&Krasnova, H. (2014). Privacy Policies and user's trust: does readability matter? Twentieth Americas Conference on Information Systems, Savannah, GA. Research paper retrieved fromhttps://www.researchgate.net/publication/262563357_Privacy_Policies_and_Users'_Trust_Does_Readability_Matter

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.

Featherman, M. S., & Wells, J. D. (2004, January). The intangibility of E-services: effects on artificiality, perceived risk, and adoption. In System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on (pp. 177-187). IEEE.

Felt, A., Egelman, S., & Wagner, D. (2012). I've got 99 problems, but vibration ain't one: A survey of smartphone users' concerns. SPSM '12, 33-44.

Forsythe, S. M., & Shi, B. (2003). Consumer patronage and risk perceptions in Internet shopping. journal of Business research, 56(11), 867-875.

Gefen, D. (2000). E-commerce: the role of familiarity and trust. Omega, 28 (6), 725-737.

Gerlach, J., Widjaja, T.,&Buxmann, P. (2014). Handle with care: how online social network providers' privacy policies impact users' information sharing behavior, J.Strateg. Inf. Syst. 24 (1), 33-34

Gilly, M.C., Graham, J.L., Wolfinbarger, M.F., & Yale, L.J. (1998). A dyadic study of impersonal information search. Journal of the Academy of Marketing Science, Vol. 26, No.2, 83-100.

Glover, J. D., Sarma, M. S., &Overbye, T. (2012). Power System Analysis & Design, SI Version. Cengage Learning.

Godes, D., &Mayzlin, D. (2004). Using online conversations to study word-of-mouth communication. Marketing science, 23 (4), 545-560.

Goel, S.,&Chengalur-Smtih, I.N. (2010). Metrics for characterizing the form of security policies, J.Strateg. Inf. Syst. 19 (4), 281-295.

Granovetter, M. S. (1973). The strength of weak ties. American journal of sociology, 1360-1380.

Gupta, S. (2013). For mobile devices, think Apps, not ads. Harvard business review 91, 70-75.

Heirman, W., Walrave, M., &Ponnet, K. (2013). Predicting adolescents' disclosure of personal information in exchange for commercial incentives: an application of an extended theory of planned behavior. Cyberpsychology, behavior and social networking, 16 (2), 81-87.

Hofstede, G. (1980). Culture and organizations. International Studies of Management & Organization, 10(4), 15-41.
ISO 690

Hone, K. &Eloff, J.H.P. (2002). Information security policy-what do international information standards say?. Computer & Security 21 (5), 402-409.

Hornyack, P., Han, S., Jung, J., Schechter, S., &Wetherall, D. (2011). These aren't the droids you're looking for: retrofitting android to protect data from imperious applications. In Proceedings of the 18th ACM conference on Computer and commuinications security.

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, 46-57.

Hu, X.,Wu, G.,Wu,Y.,& Zhang, H.(2010).The effects of Web assurance seals in consumers' initial trust in an online vendor: a functional perspective, Decis. Support. Syst. 48 (2), 407-418.

Hu. J., Chen, H.-H. &Hou T.-W. (2010). A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations, Comput. Stand. Interfaces 32 (5-6), 274-280.

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

Kelman, H. (1958). Compliance, identification, and internalization: three processes of attitude change. Journal of Conflict Resolution, 1, 51-60.

Kelman, H. (1974). Social influence and linkages between the individual and the social system: further thoughts on the processes of compliance, identification, and internalization. In. J.T. Tedeschi (Ed.) Perspectives on social power, 125-171.

Kim, D., Ferrin, D., & Rao, R. (2008). A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents. Decsion Support Systems, 44, 544-564.

Lee, M., &Youn, S. (2009). Electronic word of mouth (eWoM): How eWoM platforms influence consumer product judgment. International Journal of Advertising, 28 (3), 473-499.

Lee, Y., & Kwon, O. (2011). Intimacy, familiarity and continuance intention: an extended expectation-confirmation model in web-based services, Electronic Commerce Research and Applications 10 (3), 342-357.

Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J., and Zhang, J. (2012). Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing. In Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp'12). New York, NY: ACM Press, 501–510.

Li, Y. (2011). Empirical Studies on Online Information Privacy Concerns: Lirterature Review and an Integrative Framework, Communications of the Association of Information Systems (28:28), 453-496.

Li, Y. (2012). Theories in online information privacy research: a critical review and an integrated framework, Decision Support Systems 54 (1), 471-481.

Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. Decision Support Systems, 57, 343-354.

Lin, H.F. (2006). Understanding behavioral intention to participate in virtual communities, Cyberpsychol. Behav. 9 (5), 540-547.

Litvin, S.W., Goldsmith, R.E., & Pan, B. (2008). Electronic word of mouth in hospitality and tourism management. Tourism Management, 29 (3), 458-468.

Luhmann, N. (1979). Trust and power.

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.

Mauldin, E., &Arunachalam, V. (2002). An experimental examination of alternative forms of web assurance for business-to-consumer e-commerce. Journal of Information Systems, 16(s-1), 33-54.

McDonald, A., Reeder, R., Kelley, P., &Cranor, L. (2009). A Comparative Study of Online Privacy Policies and Formats, Privacy Enhancing Technologies, Lecture Notes in Computer Science (5672), 37-55.

Milne, G.R., Rohm, A.J., & Bahl, S. (2004). Consumers'protection of online privacy and identity. Journal of Consumer Affairs 38 (2), 217-232.

Min, J., Kim, B. (2015). How Are People Enticed to Disclose Personal Information Despite Privacy Concerns in Social Network Sites? The Calculus Between Benefit and Cost. Journal of Association for Information Science and Technology 66(4), p.839-857.

Moellering, G. (2006). Trust: Reason, Routine, Reflexivity. Knowledge Management Research & Practice, 4, 254-255.

Motiee, S., Hawkey, K., &Beznosov, K. (2010). Do windows users follow the principle of least privilege?: investigating user account control practices. In Proceedings of the Sixth Symposium on Usable Privacy and Security.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs, 41(1), 100-126.

Okdie, B. M., Guadagno, R. E., Bernieri, F. J., Geers, A. L., &Mclarney-Vesotski, A. R. (2011). Getting to know you: Face-to-face versus online interactions. Computers in Human Behavior, 27(1), 153-159

Pagano, D., &Maalej, W. (2013, July). User feedback in the appstore: An empirical study. In 2013 21st IEEE international requirements engineering conference (RE) (pp. 125-134). IEEE. ISO 690

Pahnila, S., Siponen, M., Mahmood, A. (2007). Employee's behaviour towards IS security Policy Compliance. In: Proceedings of 40th Hawaii International Conference on System Science (HICSS '07).

Pan, Y., &Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. Journal of Retailing, 82(4), 331-338.

Pavlou, P. (2003). Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. International Journal of Electronic Commerce, 7, (3), 69-103.

Pew ResearchCenter (2015). Accessed on 22/09/2016 from. Apps Permissions in the Google Play Storehttp://www.pewinternet.org/2015/11/10/apps-permissions-in-the-google-play-store/

Pollach,I. (2007) What's wrong with Online Privacy Policies? Communications of the ACM (50:9), 103-108.

Pornpitakpan, C. (2004). The Persuasiveness of Source Credibility: A Critical Review of Five Decades' Evidence. Journal of Applied Social Psychology, Vol. 34.

Rogers, E.M. (2003). Diffusion of innovations. New York, USA.

Sen, S. and 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.

Singh, R.I., Sumeeth, M., & Miller, J. (2011). A User-Centric Evaluation of the Readability of Privacy Policies in Popular Web Sites, Information Systems Frontiers (13:4), 501-514.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. MIS quarterly, 167-196.

Statista (2016). Number of apps available in leading app stores 2015. Accessed on 25/5/2016 from: ⟨http://www.statista.com/statistics/276623/number-of-appsavailable-in-leading-app-stores/⟩.

Statista (2016). Worldwide mobile app revenues 2015–2020. Accessed on 25/5/2016 from: ⟨http:// www.statista.com/statistics/269025/worldwide-mobile-app-revenue-forecast/⟩.

Van Slyke, C., Shim, J.T., Johnson, R., & Jiang, J.J. (2006). Concern for information privacy and online consumer purchasing. Journal of the Association for Information Systems, 7 (1), 16.

Tsai, J.Y., Egelman, S., Cranor, L., &Acquisti, A. (2011). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, Information Systems Research (22:2), 254-268.

Vail, M.W., Earp, J.B., Anton, A.I. (2008). An empirical study of consumer perception and comprehension of web site privacy policy. IEEE Transactions on Engineering Management 5 (3), 442-454.3

Venkatesh, V., Morris, M.G., Davis, G.B., & Davis, F.D. (2003). User acceptance of information technolog: Toward a unified view. MIS Quarterly, 425-478.

Vidas, T., Christin, N., &Cranor, L.F. (2011). Curbing Android Permission Creep.

Warkentin, M., Gefen, D., Pavlou, P., &Rose,G. (2002). Encouraging citizen adoption of e-government by building trust. Electron Markets, 12, (3), 157-162.

Westin, A. F. (1966). Science, privacy, and freedom: Issues and proposals for the 1970's. Part I--The current impact of surveillance on privacy. Columbia Law Review, 66(6), 1003-1050.

Westin, A.F.(1967). Privacy and Freedom. Athenaeum, New York.

Westin, A.F. (2003). Social and political dimensions of privacy, Journal of Social Issues 59 (2), 431-453.

Wilson, A., Zeithaml, V. A., Bitner, M. J., &Gremler, D. D. (2012). Services marketing: Integrating customer focus across the firm. McGraw Hill.

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

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

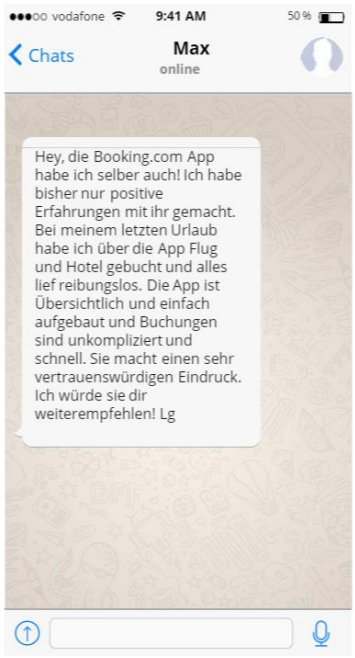
XueMei, T. and ShengQiang, L. (2014). The persuasion effect of hotel online reviews on regulatoryfocus tourist. Tourism Tribune 29 (10), 61-68.

## Appendices

Appendix A Scenarios

**Scenario 1**

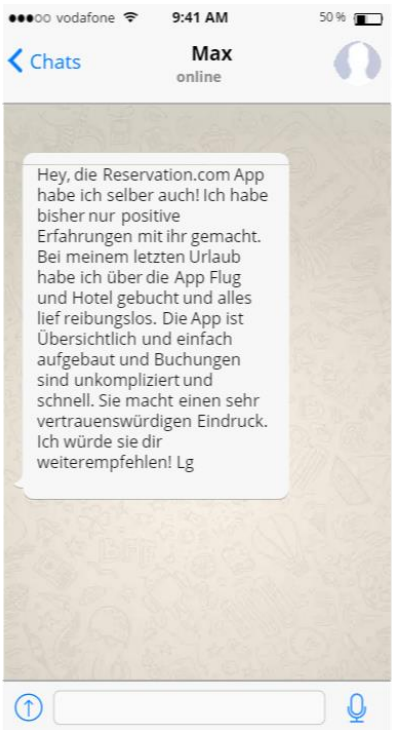
Manipulation: Fam./ Friends+;Stranger-/High Sensivity



**Scenario 2**

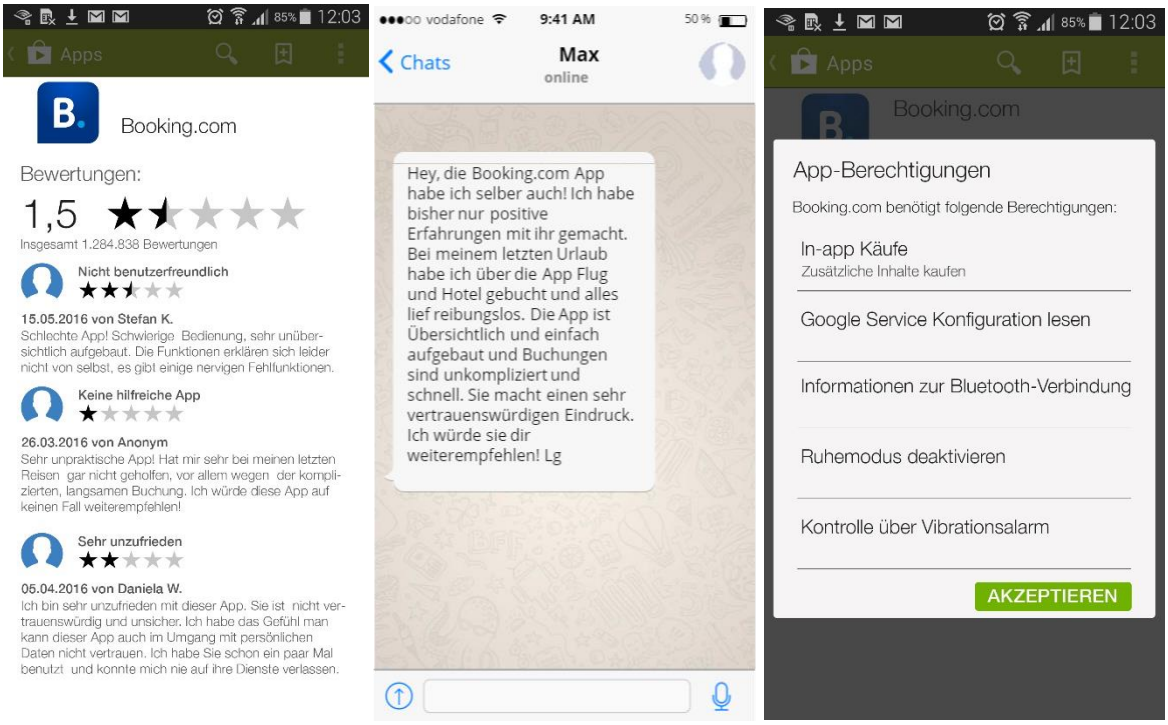
Manipulation: Unfam./ Friends+;Stranger-/High Sensivity



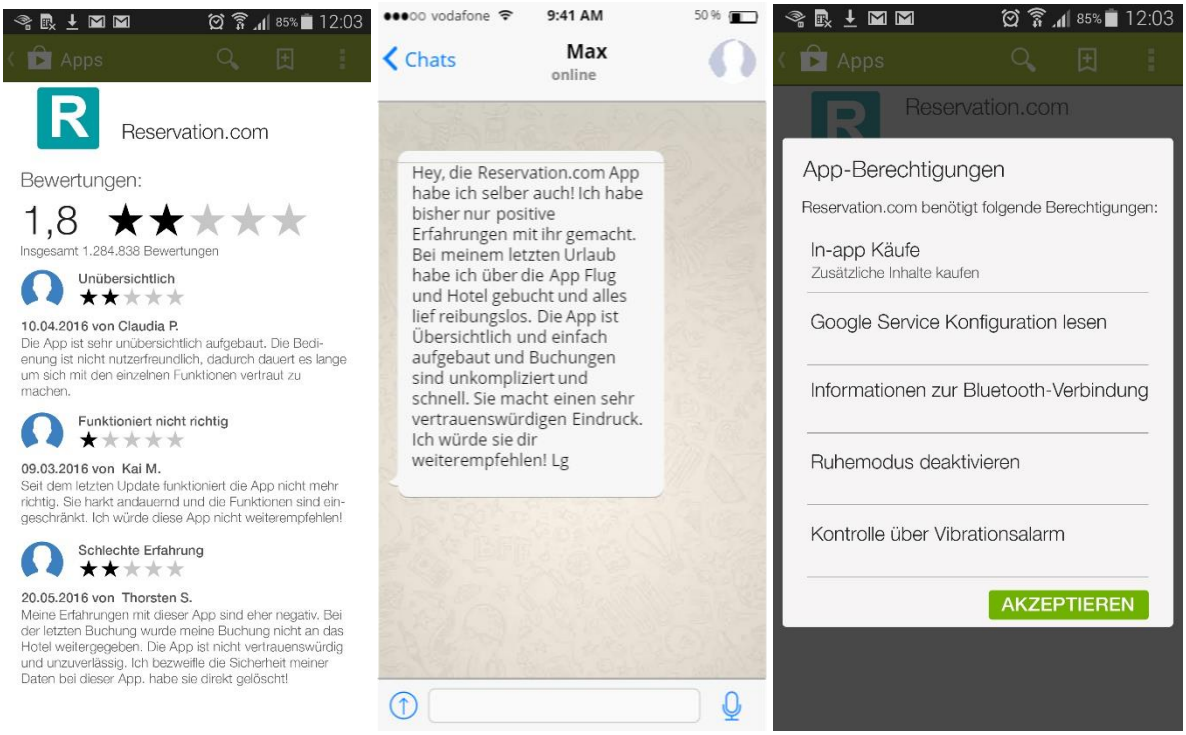
**Scenario 3**

Manipulation: Fam./ Friends+;Stranger-/Low Sensivity



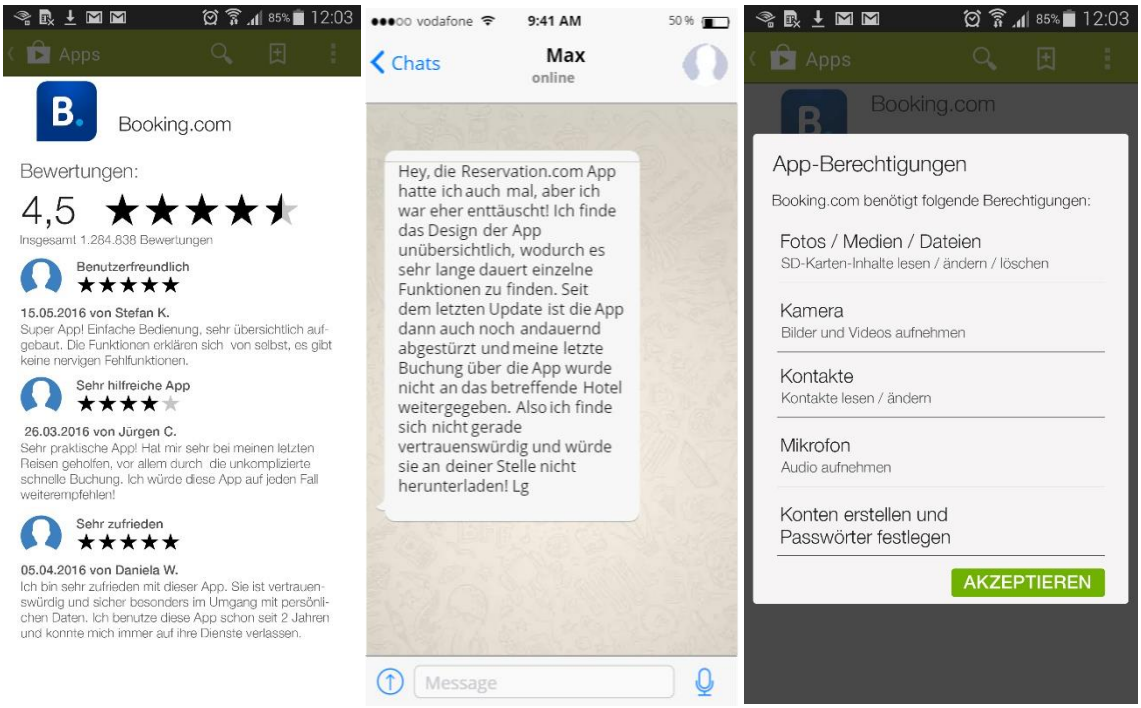

**Scenario 4**

Manipulation: Unfam./ Friends+;Strangers-/ Low Sensivity



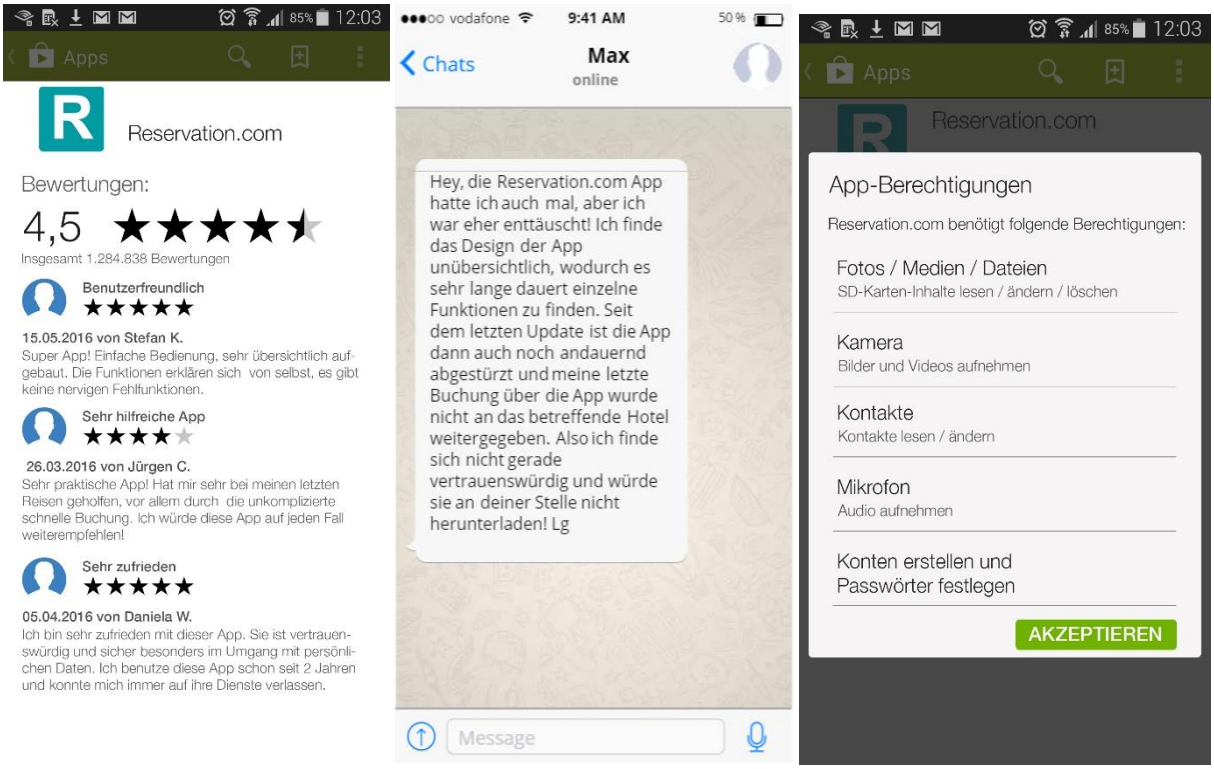

**Scenario 5**

Manipulation: Fam./ Friends-;Strangers+/ High Sensivity



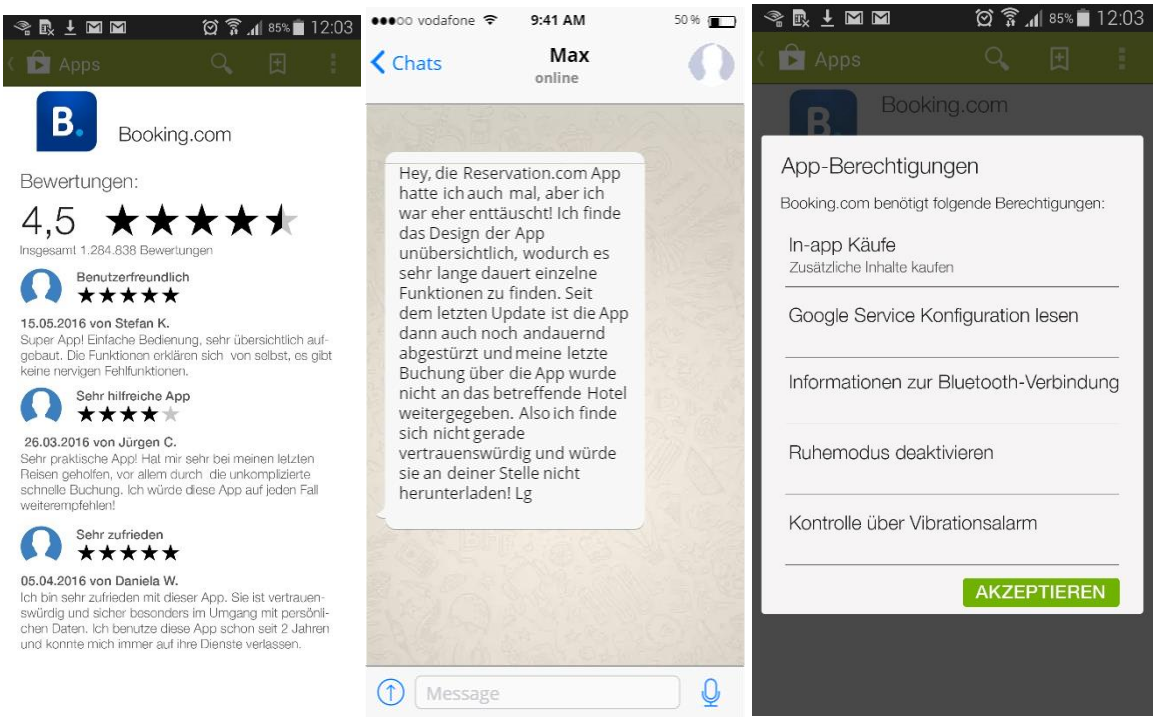

**Scenario 6**

Manipulation: Unfam./Friends-;Strangers+/ High Sensivity



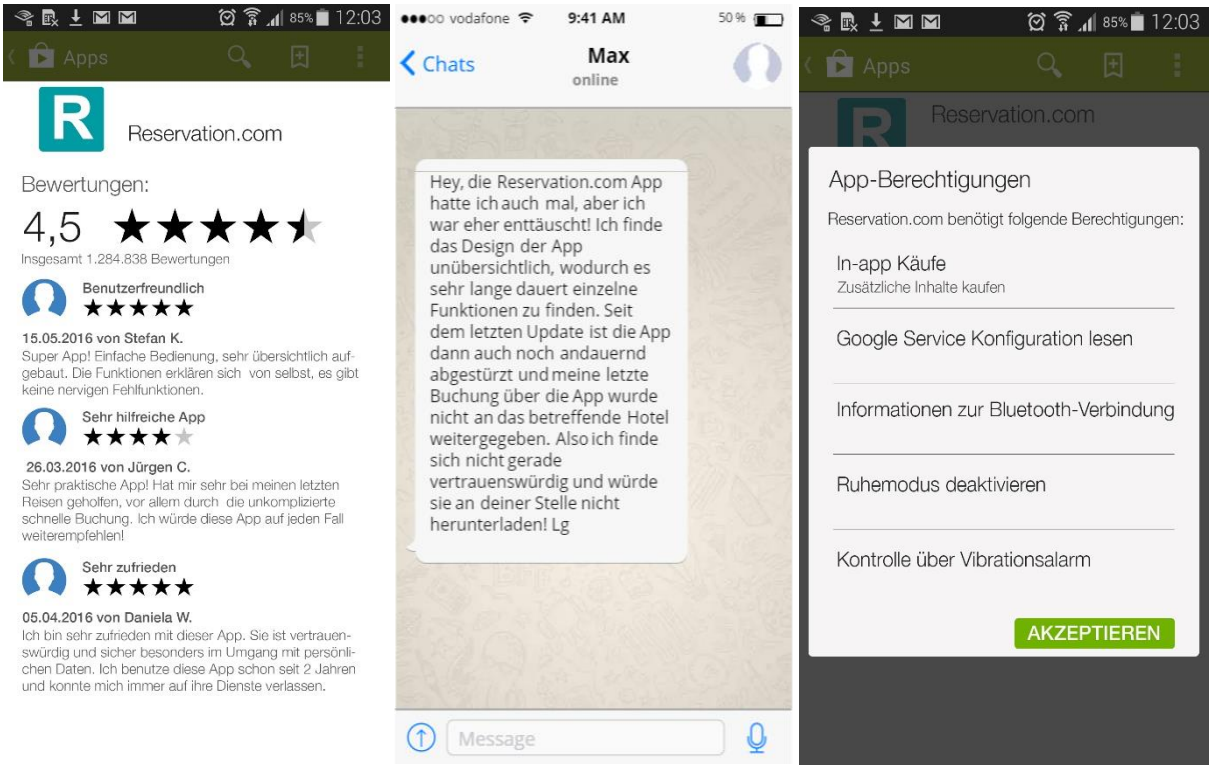

**Scenario 7**

Manipulation: Fam./ Friends-;Strangers+/ Low Sensivity




**Scenario 8**

Manipulation: Unfam./Friends-;Strangers+/ Low Sensivity




## Appendix B Survey

Original survey in German

**Introduction**

Liebe/r Teilnehmer/in,

vielen Dank für die Teilnahme an dem Abschlussprojekt meiner Masterarbeit!

In der folgenden Umfrage geht es um das Download-Verhalten im Bezug auf Apps.
Im Folgenden erhalten Sie verschiedene Informationen, bezogen auf eine App. Bitte lesen Sie die Informationen sorgfältig durch und versuchen Sie die darauf folgenden Fragen so vollständig wie möglich zu beantworten. Bei den Fragen geht es um Ihre persönliche Meinung, daher gibt es keine richtige oder falsche Antwort.

Die Antworten werden anonym ausgewertet und können nicht auf individuelle Teilnehmer zurück geführt werden. Die Umfrage dauert ca. 10 Minuten. Bei Fragen oder Anmerkungen können Sie mich gerne über die folgende E-Mail Adresse kontaktieren : l.lindemeier@student.utwente.nl

Mit freundlichen Grüßen,

Lena Lindemeier
Masterstudentin (Communication Studies) an der University of 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)

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) _____

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) _____

**General privacy attitude (Covariate )**

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 | Trifft eher nicht zu | Teils-Teils | Trifft eher zu | Trifft zu |
|---|---|---|---|---|---|
| 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) _____

**Bitte lesen Sie die folgenden Informationen sorgfältig durch und beantworten Sie die darauf folgenden Fragen:**

Stellen Sie sich die folgende Situation vor:
Sie möchten die App Booking.com herunterladen, eine App, die Ihnen dabei hilft z.B. Hotels oder Flüge zu buchen.
Um sich einen Eindruck vor dem Download zu verschaffen, sehen Sie sich zunächst die bestehenden Bewertungen von anderen Nutzern an:

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

0 ⟶ 100

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

| | | | | | |
|---|---|---|---|---|---|
| Positiv:Negativ (1) | ❍ | ❍ | ❍ | ❍ | ❍ |

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 | Trifft eher nicht zu | Teils-Teils | Trifft eher zu | Trifft zu |
|---|---|---|---|---|---|
| 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 | Trifft eher nicht zu | Teils-Teils | Trifft eher zu | Trifft zu |
|---|---|---|---|---|---|
| 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 | Trifft eher nicht zu | Teils-Teils | Trifft eher zu | Trifft zu |
|---|---|---|---|---|---|
| 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 | Trifft eher nicht zu | Teils-Teils | Trifft eher zu | Trifft zu |
|---|---|---|---|---|---|
| Diese App erscheint mir vertrauenswürdig (1) | ❍ | ❍ | ❍ | ❍ | ❍ |
| Ich habe Vertauen 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 | Trifft eher nicht zu | Teils-Teils | Trifft eher zu | Trifft zu |
|---|---|---|---|---|---|
| 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) | ❍ | ❍ | ❍ | ❍ | ❍ |