THE PRIVACY PARADOX & FRAMING EFFECTS

MASTER THESIS – BEHAVIOURAL ECONOMICS

VITA VAN DER KRAAIJ

ERASMUS UNIVERSITY ROTTERDAM

Erasmus School of Economics

-

Master Thesis

Business and Economics

Behavioral Economics

-

The Privacy Paradox and Framing Effects

-

Vita van der Kraaij

433011vk

-

Supervisor: Dr. Chen Li

Second Assessor:

I. Aydogan

-

Date final version:

31 October 2016

Date defense:

13 December 2016

Abstract

This study investigates the impact of framing effects on the willingness of online consumers to disclose personal information. Earlier research accentuated that online buyers easily reveal their private data in exchange for relatively small rewards as a newsletter or a personalized greeting. This imprudent behavior is in great contrast with the reported high levels of privacy concerns among consumers. The discrepancy between actual or intended privacy related behavior and stated privacy concern is coined as the privacy paradox.

The main objective of this study is to examine if by either positively or negatively highlighting the consequences of revealing the private information, the behavior of consumers can be influenced. Nevertheless, the results of the analyses demonstrated that it is problematic to impact the privacy related behavior of consumers. As a consequence of this conclusion, the validity of the privacy paradox is questioned. Is the postulated ambiguity between privacy concerns and intended behavior well founded? The soundness of the main premise of the privacy paradox is examined in the second part of the study and after an extensive analysis refuted. Hence, the main conclusion of this research is that the reported levels of privacy concerns are decisive for intended privacy related behavior. As a consequence, privacy related decision-making is compatible and therefore hard to influence by non-normative factors such as framing effects. This conclusion is progressive and begs for reassessment of the fundamental principle in the research on information privacy: the privacy paradox.

Keywords: privacy paradox, information privacy, behavioral economics, framing effects, endowment effect.

Table of content

1 Introduction

In the last decades, the internet has been transformed from an information-providing medium to a fundamental component of our daily live (Jenen, Potts & Jensen, 2005). Everyday, 47 billion e-mail massages are sent, 95 million tweets are submitted and 30 million pieces of content are uploaded on Facebook (Kokolakis, 2015). Besides its mean to establish social interaction, the internet is utilized by consumers to acquire divergent goods and services and last year e-commerce profits surpassed 256 billion dollar in the United States (Statista, 2016). Due to this tremendous success of the e-commerce, it is of strategic importance for retailers to gain better insights into the online behavior of their customers (Lee & Cranage, 2011). These insights enable online vendors to approach their customers in a personalized manner. As a consequence, the chef enjoys personalized discounts on the newest cookbooks whilst the football dilettante is persuaded with football related content.

This personalized approach enhances several competitive advantages as high levels of customer satisfaction and an increase in the cross-selling of products (Chellappa & Sin, 2015). Hence, the personalized marketing strategy has been found to be extremely successful which is also illustrated by the success of Google. The leading web search engine reported a net brand value of 82.5 billion dollar, an achievement that is mainly caused by the sale of detailed customer characteristics, purchase behavior, searching habits and personalized advertisement (Forbes, 2016). Not surprisingly, personal data is often termed as the oil of the internet or the new currency of the digital world (Dutta & Mia, 2011). Hence, the online vendor will devote a lot of effort to obtain the personal information of its potential customers and utilize various means to access the private data. For instance, a consumer can be rewarded with a relatively small discount in exchange for subscribing to the newsletter. Nevertheless, earlier research has accentuated that despite the efforts of the retailer, online consumers easily reveal their personal information and do not require a big compensation (Acquisti, 2004; Baek, 2014; Norberg, 2007). This abundant disclosing behavior is at least remarkably. Several polls have indicated that online consumers exhibit high levels of privacy concerns and they value information privacy. This discrepancy between the stated privacy concerns and actual privacy related behavior has been coined as the privacy paradox (Norberg, 2007). The main premise of the paradox stresses that the stated privacy concerns of consumers are not explanatory for their actual nor intended privacy related behavior (Norberg, 2007; Smith et al., 2011).

Findings in behavioral economic showed that people often exhibit inconsistency in their behaviors and that their decisions can be influenced by factors that are hard to justify on a normative base. For instance, decision makers respond inconsistently to choices that are objectively the same, but formulated differently (Kahneman & Tversky, 1984). Hence, by highlighting different aspects of the same concept, choices can be influenced. This method is coined framing and the impact has been found to be very powerful. Information is often framed in positive or negative terms, to enhance either the favorability or the unattractiveness of an object (Levin & Gaeth, 1988).

It is intriguing to investigate if framing effects can impact the willingness to consumers to disclose personal information for two reasons. On the one hand, utilizing framing effects can benefit the online vendor as priming the benefits of disclosing can elicit positive associations among the consumer. Consequently, due to these positive associations the consumer might become more willing to disclose private data. On the other hand,

framing effects might impact the reckless behavior of consumers and overcome the discrepancies between the high levels privacy concerns and actual imprudent behavior. As stated, consumers easily disclose their personal information. In addition, current privacy regulations fail to protect consumers from this risky behavior as the regulations assume some sort of conservative behavior due to the high levels of privacy concerns that are reported. By negatively priming the disadvantages of revealing personal information, online consumers might exhibit more thoughtful behavior.
Based on a consolidation of above the following research question is formulated:

How can framing effects influence consumers' willingness to disclose personal information in an e-commerce environment?

An online questionnaire is conducted to gather the data required to formulate an adequate answer to the main inquire of the thesis. Nevertheless, a preliminary theoretical examination is required to develop a sufficient questionnaire. Therefore, the relevant concepts as the privacy paradox and the different non-normative factors that impact the privacy related decision making of consumers will be discussed in length in the next chapter. Afterwards, the concepts of choice architecture and framing will be described in more detail. Afterwards, the research design of the experiment will be discussed: which hypotheses will be tested and how is the required data gathered? Subsequently, the results of the analyses are described in detail and conclusions regarding the hypotheses are drawn. In the final part of the thesis, a general conclusion is formulated and discussed in detail and recommendations for further research are given.

2 Literature Review

The main objective of this thesis is to examine if the willingness of online consumers to disclose personal information can be affected. Traditional studies understood this decision as the outcome of a deliberate cost-benefit analysis, i.e. as the result of the privacy calculus. Nevertheless, contemporary research has accentuated several inconsistencies in privacy related behavior and therefore considered the calculus to be inaccurate. The ambiguities are comprehended by the privacy paradox and various studies have attempted to clarify the paradox. The aim of this chapter is to examine the privacy calculus, its features and its flaws. After this, the privacy paradox and the corresponding theories that try to explain the paradox are discussed. Finally, the concept of framing effects is considered.

2.1 A standard economic interpretation: the privacy calculus

Due to the tremendous success of the internet and e-commerce, a voluminous amount of personal information of online consumers is collected, registered and processed every second of a day. Leading companies operating in divergent industries accentuate on the potential of analyzing customer data and are using these consumer insights to gain competitive advantages (Graeff & Harmon, 2002; McGuire, Manyika & Chui, 2012; Orenga-Roglá & Chalmeta, 2016). Nevertheless, these insights are obtained in devious ways and a number of reputable firms such as Google (Hansell, 2008a; Hansell, 2008b), Facebook (Stone & Stelter, 2009) and Amazon.com (Hinz, Hann & Spann, 2011) have been criticized for their questionable privacy policies in recent years. For instance, the e-commerce giant Amazon.com adopted a price discrimination strategy based on the personal preferences and characteristics of their consumers (Hinz et al., 2011). A consequence of this negative media coverage is that it evoked a privacy related consensus among consumers. Hence, several polls have indicated that online consumers obtained increasing information privacy concerns and highly appreciate information privacy (Westin, 2001). A poll among American consumers indicated that 72% of the respondents are highly concerned that their information privacy in an online setting is violated (Consumers-Union, 2008). This specific type of privacy refers to the "ability of individuals to control when, how and to what extent their personal information is exchanged with and used by others" (Li, Sarathy & Xu, 2010, p. 63). In addition, numerous contemporary studies have elucidated that information privacy concerns are one of the major obstacles that make consumers reluctant to shop online (Li, Sarathy & Xu, 2011; Smith, Dinev & Xu., 2011; Phelps, Nowak & Ferrell, 2000). For instance, Phelps et al. (2000) advocated that online transactions are impeded by the unwillingness of some consumers to share their personal information with e-retailers. Therefore, an understanding of the various facets that affect the willingness of consumers to share their personal information is needed to ensure a further development of e-commerce (Gefen, Karahanna & Straub, 2003).

2.1.1 The privacy calculus

The privacy calculus model is the predominant model that examines factors that impact personal information disclosure (e.g. Culnan & Armstrong, 1999; Dinev & Hart, 2006; Kehr, Kowatsch, Wentzel &

Fleisch, 2015; Li et al., 2010; Li et al., 2011; Xu, Luo, Carroll & Rosson, 2011). The model views information privacy as a commodity, i.e. an economic good that can be traded for other goods and services (Kehr et al., 2015; Smith, Milberg & Burke, 1996). This interpretation argues that even though people are generally concerned about their information privacy, they are willing to trade (some of their) personal information in exchange for certain benefits as financial advantages (Xu, Dinev, Smith & Hart, 2008), personalization (Chellappa & Sin, 2005) and social benefits (Debatin, Lovejoy, Horn & Huges, 2009). Therefore, privacy related choices are affected in a twofold manner: positively affected by the expected utility of the anticipated benefits and negatively affected by the potential loss of privacy violation (Culnam & Armstrong, 1999; Dinev & Hart, 2006). The choice to share personal information can then be understood as a decision making process guided by a cognitive assessment of the tradeoff between potential costs and benefits of private information disclosure. For instance, divulging personal information to an online bookstore may generate a direct discount on a purchase. On the other hand, revealing the data might provokes price discrimination and as a consequence unwanted expenses. The privacy calculus assumes that individuals outweigh these costs and benefits and behave in ways that maximize the overall net utility gain (Culnan & Armstrong, 1999; Culnan & Bies, 2003; Dinev & Hart, 2006).

The calculus was originally formulated by Culnan and Armstrong (1999) but adjusted by Dinev and Hart (2006) to the context of online transactions. In this altered model, the main principle (i.e. the willingness of consumers to reveal personal information is the decisive of a cost-benefit analysis) remained unchanged. Dinev and Hart (2006) described the polarities as the "Perceived internet Privacy Risk" and "Personal internet Interest." In addition, the authors defined risk as the "the possibility of loss that is an inherently subjective construct" (Dinev & Hart, 2006 p. 63). On the other side of the calculus, the "Personal internet Interest" refers to the benefits or revealing personal information in an online environment. These benefits are described as "the cognitive attraction to the internet interactions" (Dinev & Hart, 2006 p.68) and vary from pleasure to usefulness. Many studies adopted the privacy calculus and examined the model in different online contexts as the internet in general (Malhotra, Kim & Agarwal, 2004), e-commerce (Li et al., 2010; Li et al., 2011) and mobile applications (Kehr et al., 2015; Xu et al., 2011). Most studies however, adjusted the original constructs as proposed by Dinev and Hart (2006) and made the antecedents suitable to their own research objective. Nevertheless, the original cost-benefit analysis remained unaltered.

The privacy calculus thus accentuates that people can choose to bargain personal information in exchange for divergent benefits, as long as the decision maximize the net overall utility gain. To constitute a comprehensive understanding of the privacy calculus both the benefits and costs of revealing personal information will be discussed.

2.1.2 The benefits of sharing personal information online

The advantages of sharing personal information in an online setting are divergent. Earlier studies have emphasized three major benefits of disclosing personal data in an online environment. These advantages are: financial awards, social benefits and personalized services and offers. Various studies examining privacy in an online setting have identified that compensating consumers by offering financial awards encourage revealing personal information (Hann, Hui, Lee & Png et al., 2007; Huberman, Adar & Fine; 2005; Phelps et al., 2000).

Nevertheless, scholars hold differing opinions on the suitable reward and found different valuations for the same type of personal information. For instance, Huberman et al. (2005) found that the average demanded price for revealing age was $57.56 whilst another study by Carrascal et al. (2013) estimated the price for disclosing age, gender, address and salary to be €25 (approx. $28.00). Other studies emphasized on the social benefits of revealing personal information (Debatin et al., 2009; Lee, Park & Kim, 2013). These social benefits are defined as the establishment of social identity and social relationships by interacting with certain social groups by using social networks (Debatin et al., 2009).

Nevertheless, many studies have agreed that personalized offers and services are the biggest advantage of disclosing personal information in an online environment for consumers (Awad & Krishnan, 2006; Lee & Cranage, 2011; Tam & Ho, 2005). In addition, obtaining detailed insights customer characteristics as preferences and buying behavior can reward the online vendor with several competitive advantages. Therefore, online retailers try to persuade their consumers by offering personalized services and discounts to reveal their private information.

In the context of e-commerce, personalization refers to the "tailoring and recommending products and services according to specific consumer characteristics (e.g. browsing/purchasing preferences and demographics) before a consumer begins the search for a product" (Lee & Cranage, 2011 p. 998). Hence, personalization is an efficient marketing strategy designed to target individual consumers (Alatalo & Siponen, 2001; Lee & Cranage, 2011). The personalization strategy is implemented through Customer Relationship Management tools and sophisticated data mining techniques (Chellappa & Sin, 2005). The main objective of these intelligence instruments is to acquire consumer insights. Subsequently, these insights on preferences and characteristics enable online retailers to segment their customers in different target groups and create customer profiles. This segmentation then allows retailers to address their customers with a one-by-one approach and result in a higher level of customer satisfaction and an improved customer retention rate (Challappa & Sin, 2005). Obtaining detailed insights in customer profiles can therefore culminate in major competitive advantages. For instance, it can increase the cross-selling of specific products by offering customers a discount on correlated products inspired by the purchase history of previous customers (Challappa & Sin, 2005). Obtaining detailed customer insights is therefore a strategic priority of online vendors (Lee & Cranage, 2011).

On the other hand, the personalization strategy can benefit the customer in many different ways. For instance, the customer can feel appreciated and welcome by a personalized greeting on the webstore's home-screen (Sundar & Marathe, 2010). In addition, several default functions as shipping address, payments methods and delivery options can increase convenience of the shopping experience (Alatalo & Siponen, 2001). Another, more advanced, form of personalization is to send personalized notifications to inform the customer on the availability of a preferred product or relevant marketing actions to the customer e-mail address or mobile device (Chellappa & Sin, 2005). By analyzing the collective behavior of an entire customer database, online retailers can personalize the entire shopping experience of consumers by tailoring recommendations and promotions. Therefore, disclosing personal information can reward the online consumer with convenience and financial benefits. Chellappa and Sin (2005) found that these benefits of personalization could overweigh the harm of privacy concerns. In other words, people are willing to overcome their privacy concerns and choose to disclose their personal information in exchange for the convenience and financial benefits of a personalized shopping experience (Alatalo & Siponen, 2001; Chellappa & Sin, 2005; Lee & Cranage, 2011).

Hence, it is on the one hand of strategically importance for the online vendor to obtain detailed insights in customer profiles. This information can enhance competitive advantages and can increase, for instance, the cross-selling on a website by personalized offers. As a consequence, the online vendor will devote great effort to obtain the personal information of customers. On the other hand, by utilizing personalized services and offers, the customer gains several advantages of disclosing personal information. Hence, the customer is rewarded with convenience and financial benefits in exchange for disclosing the personal information.

2.1.3 The costs of sharing personal information online

Various studies have identified several risks of sharing personal information in an online setting, which harmonize under the category of information privacy violations (Cho, Rivera-Sánchez & Lim, 2009. Dinev and Hart (2006) have found several sources of organizational opportunistic behavior that influence the perceived risks of consumers, including providing personal information to third parties, unauthorized access and fraud. In addition, Dinev and Hart (2006) articulated the relationship between the costs of revealing personal information and privacy concerns. A person that perceives high internet risks is assumed to have high information privacy concerns. Many studies have adopted this concept of internet privacy concerns as main risk antecedent (Bélanger & Crossler, 2011; Malhotra et al., 2004; Milberg, Smith & Burke, 2000; Spiekermann, Grossklags & Berendt, 2001). Internet privacy concerns refer to "the individuals' perceptions of what happens with the information they provide via the Internet" (Bélanger & Crossler, 2011 p. 1020). The level of information privacy concern is therefore a construct that is measured by a questionnaire. Furthermore, information privacy concerns are acknowledged to negatively affect the users' willingness to disclose personal information (Bélanger & Crossler, 2011; Dinev & Hart, 2006; Hui, Tan & Gho, 2006; Malhotra et al., 2004; Smith et al., 2011; Xu et al., 2008).

Several demographical variables have been found to influence the privacy concerns of consumers. For instance, Xu et al. (2008) has emphasized that young consumers are less likely to be concerned about information privacy. Individuals that achieved higher level of education are found to be more concerned about online privacy than those with lower levels of education completed (Cho et al., 2009; Sheehan, 1999). Other studies (Sheehan, 1999; Youn & Hall, 2008) have found that women are generally more concerned about information privacy compared to men. Smith et al. (2011) highlighted that prior privacy experience influences the privacy concerns of consumers. According to their research, consumers that have been exposed to privacy abuses or have been a victim of privacy violations possess higher privacy concerns. Furthermore, research has accentuated that the privacy concerns of consumers are triggered when consumers notice that online vendors are collecting and or using their personal information without their permission (Smith et al., 2011 & Phelps et al., 2000). However, when vendor ask their customers permission to use their personal information, consumers are less concerned about their privacy (Smith et al., 2011).

2.1.4 Privacy statements

Following these results, many online retailers express several privacy statements on their website. These statements usually detail how the online vendor intends to collect the personal information of the consumer and how this data is collected, processed and used (Vail, Earp & Antón, 2008). The United States has

currently not adopted a single overarching privacy protection law (Baumer, Earp & Poindexter, 2004). Expectations include protection for healthcare data, financial information and restrictions on information obtained for children. Nonetheless, most American commercial websites display a privacy policy statement, presumably to enhance the trust of their customers (Baumer et al., 2004). These privacy statements inform the consumers how their personal data is collected and processed and then leave the option to the consumer to decide to continue shopping on the website or not. This policy is in line with the conceptualization of privacy as a commodity (Smith et al., 2011).

Various studies have investigated the effect of privacy statements on the willingness of consumers to reveal personal information online. It is accentuated that consumers are often reluctant to read the privacy statements and the trustworthiness of the website is enhanced by just the presence of such declaration (Meinert, Peterson, Criswell & Crossland, 2006; Pan & Zinkhan, 2006). The content of privacy statements is therefore irrelevant. Privacy statements thus fail to inform the online consumers in a proper manner. Just by their presence they (untruthfully) enhance the trust of the consumer and subsequently increase the willingness of consumers to disclose personal information (Beldad, de Jong & Steehouder, 2009; Xie, Teo & Wan, 2006).

In sum, the traditional research on information privacy advocates the privacy calculus model. This model assumes that individuals' choice to reveal personal information is the outcome of a sensible cost-benefit analysis. Earlier studies have identified several risks antecedents of divulging personal data as unauthorized access and fraud. These risk perceptions are generally harmonized in the concept of privacy concerns. Personalization of shopping experience is on the other hand acknowledged to be the biggest advantage of disclosing. To enhance the trust of consumers, online retailers exhibit several privacy statements on their websites. These privacy statements are noted to have a positive influence on the consumers' willingness of revealing personal information despite of the actual content.

2.2 The privacy paradox

As elaborated in the previous section, the privacy calculus is a primary instrument utilized in several studies that examined information privacy. This model typically regards consumers' intention to reveal personal information as an outcome of a delicate assessment between the perceived risks and apparent benefits. An individual with considerable privacy concerns will value the costs of revealing personal information relatively high and is therefore assumed to be less willing to reveal personal information. Earlier studies have emphasized this relationship in different contexts, as a general offline setting, e-commerce transactions and mobile applications. Nevertheless, there are reasons to believe that privacy related decision-making is not as consistent as the privacy calculus assumes. A numerous amount of research criticized the dominant hypothesis of the privacy calculus which implies that the level of privacy concerns negatively influence the willingness to reveal personal information (e.g. Acquisti, 2004; Acquisti and Grossklags, 2005; Barnes, 2006; Beresford, Kübler & Preibusch, 2012; Brown, 2001; Carrascal et al., 2013; Egelman, Felt & Wagner, 2013; Hann et al., 2007; Hughes-Roberts, 2013; Norberg, Horne & Horne, 2007; Spiekermann et al., 2001; Zafeiropoulou, Millard, Webber & O'Hara, 2013). As opposed to the privacy calculus, these studies claimed that that stated privacy concerns are not explanatory for the stated intention to disclose personal information.

Recent studies indicated that consumers are highly concerned about their information privacy and thus collection and usage of their personal information (Pew Research Center, 2014). Nevertheless, an examination of actual privacy related behavior shows that individuals reveal their personal information for minuscule awards, e.g. the attention of others participating in a social network (Barnes, 2006) or relative small monetary awards (Carrascal et al., 2013). This inconsistency has been studied extensively in the last decades. One of the first studies that examined this inconsistency was by Syre and Stein (2001) They researched the use of loyalty cards in supermarkets and found, contrary to what might be expected due to the general high privacy concerns of consumers, that consumers were eager to trade personal information in exchange for relatively small discounts. However, this preliminary research did not measure the privacy attitude of the respondents and simply assumed the general privacy concerns to be high. Spiekermann et al. (2001) on the other hand, utilized a multivariate technique to cluster their respondents into three different segments. By answering several privacy related questions, each person was categorized into different segments. Inspired by the privacy calculus, the research hypothesized that the level of privacy concerns defines the willingness of revealing personal details in an online environment. However, they found no differences in levels of disclosure among the three privacy clusters. Hence, a privacy fundamentalist, i.e. a person that indicated to care a lot about privacy and expresses particular concern over losing control of personal information or others gaining unauthorized access to it, revealed as much information as respondents that were labeled as "marginally concerned". The study thus concluded that: "even though internet users have high privacy concerns, they do not act accordingly" (Spiekermann et al., 2001 p. 8).

After these pioneering studies, various researchers continued to examine the dichotomy between privacy concerns and privacy related behavioral intentions. Norgberg et al. (2007) have denoted this dichotomy as the privacy paradox. In their twofold study the researchers questioned the willingness of respondents' to disclose specific types of personal information. In the second phase of the study, that they ran 12 weeks later, the subjects were asked to actually provide these same types of personal information to a "market researcher that was not acquainted with the researchers' university. This particular condition was added to the experiment to eliminate possible feelings of trust regarding the university. The findings of the experiments accentuated that individuals disclosed a significantly greater amount of personal data compared to their stated intentions. Therefore, they concluded that "in the realm of privacy, attitude and concerns may not be accurate predictor of actual behavior and other explanations should be sought" (Norgberg et al., 2007 p. 118). In their highly cited paper Smith et al. (2011) refer to the privacy paradox as follow: "Despite the reported high privacy concerns, consumers still readily submit their personal information in a number of circumstances" (Smith et al., 2011 p. 993). Hence, individual concerns on information privacy are inadequate predictors of individual intended or actual privacy related behavior.

Numerous studies support the main hypothesis of the privacy paradox and found low and non-significant correlations between privacy concerns and intended or actual privacy related behavior (e.g. Acquisti, 2004; Acquisti and Grossklags, 2005; Barnes, 2006; Beresford et al., 2012; Brown, 2001; Carrascal et al., 2013; Egelman et al., 2013§; Hann et al., 2007; Hughes-Roberts, 2013; Norberg et al., 2007; Spiekermann et al., 2001; Zafeiropoulou et al., 2013). For instance, Beresford et al. (2012) conducted a field experiment in which participants were asked to buy a DVD from one of the two DVD retailers. The shops of the DVD vendors were almost identical and only differed in a single detail. When a consumer intended to buy a DVD in the first shop,

the shop assistant asked the customer to reveal his income and his date of birth. Contrary, in the other shop the customer was asked to disclose his favorite color and his date of birth. It is evident that the information requested by the first retailer is more sensitive. Nevertheless, with equal prices in the two different shops, the sales in both stores were the same. When the prices reduced €1 in the first store, almost all subjects chose to buy the DVD in the cheaper store, regardless of the requested sensitive information. In addition, a post-experiment questionnaire examined the privacy concerns of the subjects. 75% of the respondents indicated to have high privacy concerns and additionally 95% said to value personal information.

The privacy paradox has been examined in many different contexts. For instance, Tufecki (2008) has analyzed the effect of privacy concerns on personal data disclosure on social media networks. The study had found no relation between online privacy concerns and information disclosure. Furthermore, the study of Zafeiropoulou et al. (2013) researched the disclosure of location data, a type of personal information collected and processed by mobile applications. Likewise, the study found no relationship between privacy concerns and the disclosure of personal information and thus supports the privacy paradox.

Contiguous to the privacy paradox there is another contradiction known in the information privacy field of research, i.e. the personalization paradox (Awad & Krishnan, 2006; Bleier & Eisenbeiss, 2015; Lee & Cranage, 2011; Xu et al., 2011). Even though this paradox is less prominent in the contemporary debate on information privacy, it likewise points out the inconsistency of online consumers. As elaborated on the previous section, the marketing strategy personalization creates divergent advantage. However, it inherently requires consumers to reveal personal information (Lee & Cranage, 2011). Therefore, personalization strategies might provokes customers concerns over their information privacy and enhance negative feelings on their personal information being collected and circulated. For instance, earlier research have emphasized that customers tend to feel that their privacy has been violated once they notice that their shopping lists are personalized based on purchase and browsing history (Lee & Cranage, 2011). The personalization paradox thus indicates that even though customers value personalized services, the personalization strategies provokes consumers concerns over their personal data being tracked, processed and circulated. Due to privacy concerns, consumers are not willing to reveal personal information and this reluctance impede the personalization strategies.

As a conclusion it can be stated that privacy related behavior of online consumers is not as consistent as the privacy calculus assumes. Various studies have accentuated that consumers often exhibit behavior that is inconsistent with their stated privacy concerns. Therefore, the reported privacy concerns of consumers are highly unreliable for predicting the privacy related behavior. Nevertheless, it is substantial to comprehend the paradox and its underlying causes. The privacy regulations of the United States are endorsed by these generally high concerned public opinions and consistent with the privacy calculus assumes some sort of cautiousness (Baumer et al., 2004). In addition, online retailers are not obliged to display privacy statements on their website and consumers often are reluctant to read those statements.

However, as the there is a dichotomy between the privacy concerns and behavior, the (lack of) regulations might fail to protect the consumer. On the other side, current privacy strategies of private companies might be too conservative as they are established on the high levels of concerns and not in accordance with the

actual behavior of consumers. This exaggeration can discourage the dot.com economy (Baek, 2014; Berger, 2010). Hence, an understanding of the privacy paradox and its causes are essential to overcome the inaccuracy.

2.3 A behavioral explanation of the privacy paradox

The privacy paradox postulates that the privacy concerns of individuals are not explanatory for their privacy related intentions nor behavior. A various amount of studies have found that consumers are highly concerned about information privacy violations, but nevertheless exhibit risky behavior by divulging personal characteristics. Therefore, a dichotomy between stated attitude and stated intentions or actual behavior is acknowledged. When the choices and actions of an individual correspond to the attitude of a person, the individual is said to exhibit consistent behavior. However, earlier studies have proven, just as the privacy paradox emphasizes, that people are not perfectly consistent and their behavior is often inconsistent with their stated attitude (e.g. Tversky & Kahneman, 1975; Tversky & Thaler, 1990; Kahneman et al., 1991). People are often biased, make inconsistent decisions and utilize a tremendous amount of heuristics to simplify the complex choices that they face. The field of research that studies these inconsistencies of human behavior in an economic context is behavioral economics. The main objective of behavioral economics is "to improve the explanatory power of standard economic theories by giving them a sounder psychological basis" (Wilkinson & Klaes, 2012 p.29). The premises and insights of behavioral economic theories are utilized to gain a better understanding of the privacy paradox in the following paragraphs.

2.3.1 Bounded rationality, heuristics and biases

Several scholars have deliberated the principles of behavioral economics to gain a better understanding of the privacy paradox. Acquisti (2004) stressed that it could be questioned whether people are able to adequately assess the drawbacks of sharing personal information as the possible advantages of revealing. Due to the advancements in information technology, the collection and usage of personal information is often invisible. Online consumers might be unaware that their personal information is gathered and used. As a result of their ignorance, people might underestimate the potential costs of visiting a website. Hence, an obvious source of information privacy uncertainty arises from incomplete and asymmetric information (Kokolakis, 2015). Moreover, even if the consumer is aware that his personal data is acquired and used it might be puzzling to estimate the (indirect) expenses (Acquisti, 2004). For example, how to adequately value the costs associated with an identity theft? What are the chances the theft actually occurs? There are reasons to question the cognitive capability of individuals to assess the likelihood of an uncertain event. The combination of imperfect information and limited cognitive capabilities is comprehended by the concept of bounded rationality (Simon, 1982). To overcome this bounded rationality people rely on mental short cuts or heuristics to simplify the complex choices that they have to make. An example of such a short cut is the availability heuristic. Tversky and Kahneman (1975) stressed that in some situations individuals assess the probability of an event by the ease with which incidents could be remembered. The reliance on availability leads to predictable biases and might be applied while evaluating the complex choices related to information privacy. For instance, an alarming news article on identity theft might inaccurately influence the evaluation of an individual and leads to an overestimation of the probabilities.

An example of a mental shortcut that is utilized in the information privacy related decision-making is the affect heuristic (Slovic, Finucance, Peters & MacGregor, 2002). The affect heuristic represents the reliance on a mental gimmick, i.e. the affective impressions, to make quick decisions. However, an undesirable consequence of the affect heuristic is that "people tend to underestimate risks associated with things they like and overestimate the risks of things they dislike" (Kokolakis, 2015 p.8). Kehr et al. (2015) examined the impact of on an interface that elicits positive affects on perceived risk of information disclosure. The study emphasized that people are more willing to reveal personal information to a website that provokes positive feelings compared to the negative interfaces. Sundar, et al. (2013) conducted an experiment in accordance with this reasoning and examined the influence of the fuzzy-boundary and the benefit heuristic. To test the impact of these heuristics, they showed one group of participants a video that accentuated on the benefits of revealing personal information online (i.e. the benefit condition). On the contrary, the other group viewed a video that illustrated how certain companies misused personal information (i.e. the fuzzy-boundary condition). After watching the videos both groups were asked to complete a questionnaire. The results indicated that the group primed with the fuzzy-boundary condition was significantly less likely to disclose personal information compared to the individuals with the benefit heuristic. Cho, Lee and Chung (2010) have researched the effect of the optimism bias on privacy related behavior. The optimism bias refers to "the consistent tendency of individuals to believe that they are less at risk of experiencing a negative event compared to others" (Kokolakis, 2015 p.8). The study of Cho et al. (2010) stressed that individuals display a strong optimism bias about online privacy risks and judge themselves to be less vulnerable to the risks of revealing personal information compared to others. Beak (2014) confirmed that people tend to underestimate the chance of information privacy infringement. In addition to the findings of Cho et al. (2010), their study accentuated that this optimism bias is positively related to the willingness of disclosing personal data.

2.3.2 Choice architecture and framing effects

The presence of the described heuristics and biases accentuates that the privacy related behavior are not as stable nor as internally consistent as often is believed. In addition, earlier studies have accentuated that inconsistent behavior can be influenced by factors that are hard to justify on normative base. As a consequence, there is the opportunity to guide the privacy related behavior of consumers. The context in which privacy related choices are presented can have a decisive effect on the behavior of consumers. In the research field of behavioral economics this phenomenon is known as the framing effect, meaning that choices can be presented in a way that highlights certain aspects of a decision and thus appeal differently to the decision maker. Hence, framing effects can influence the choices of consumers (Kahneman & Tversky, 1979; Kahneman & Tversky, 1984).

Thaler and Sunstein (2008) advocated that the choices of individuals are affected and introduced the term choice architecture. This theory refers to the phenomenon that the choices that individuals make are influenced by the way in which choices are presented. The authors stressed that a good rule of thumb is to assume that "everything matters" and hence even the smallest seemingly insignificant details influence peoples' behavior (Thaler, Sunstein & Balz, 2012). A choice architect is then the person that has the responsibility for organizing the context in which people make their choices. There are many different types of choice architects, e.g. the

doctor that describes treatments to his patients or the manager that develops the menu of a restaurant (Thaler et al., 2012). Their influence on the choices of consumers should not be underestimated. In addition, Thaler et al. (2012) elucidated the basic principles of effective choice architecture. As an example, they named defaults and stated that for every given choice there is a default option. This is the option that will obtain if the chooser does nothing. Furthermore, this default option can suggest that it represents the normal or even recommended course of actions (Thaler et al., 2012). Choice architects utilize these defaults options in divergent field and the effect is known to be powerful. An example is the default option of double printing that saved the Barack Obama's presidential campaign more than $41,000 a year (Simon, 2008).

Apart from this default option, there are many different ways to influence the choices of individuals and a well-known technique is framing (or also named priming). This method assumes that individuals choose between alternatives by weighing the pros and cons of different attributes (Levin, Schneider & Gaeth, 1998). As a consequence, choice architects can influence the behavior of people by accentuating certain features and make these more salient. This method is coined as attribute framing (Levin, Schneider & Gaeth, 1998). Within this technique, the positive framing effects accentuate the advantages of certain property while the negative labels emphasize on the negative aspects. Positive framings are acknowledged to evoke positive associations while negative labels elicit negative feelings. In addition, positive associations result in more favorable responses compared to the negative ones. An experiment that utilized this technique examines the preference of consumers for ground meat. Levin and Gaeth (1988) identified that individuals tend to prefer meat that was labeled as 75% lean and hence positively framed, compared to the negatively framed beef that was promoted as 25% light.

A few studies have examined the influence of framing effects on peoples' privacy related (intended) behaviour. For instance, Knijnenberg and Kobsa (2013) negatively primed the privacy concerns of their respondents before requesting for their willingness to reveal personal data. The results accentuated that the primed respondents exhibited a more conservative disclosing intentions. Furthermore, Johnson et al. (2002) examined the influence of the default effect. If the personal information of the respondents is already filled in by an advanced default function, people are reluctant to erase this information and easily reveal their data.

2.3.3 The disparity between Willingness-to-accept and Willingness-to-pay and the endowment effect

Besides the impact of heuristics, biases and framing effects, studies have explored the influence of psychological ownership on intentions of disclosing (Kehr et al., 2015) as well as actual disclosing (Acquisti et al., 2014) of personal information. Standard economic theory (i.e. the Coase theorem) assumes that ownership or entitlement should not affect the value of a good (Wilkinson & Klaes, 2012). In addition, general economic theories stresses that buyers and sellers should not differ on their average demand prices for the same good. This means that the Willingness-to-Accept (WTA) of sellers should not differ from the Willingness-to-Pay of buyers (WTP) (Wilkinson & Klaes, 2012). Nevertheless, many anomalies have been demonstrated. For instance, studies have identified that the WTA for hunting or fishing permits are varying from 2.6 to 16.5 times as large as the WTP of the purchasers (Horowitz & McConnell, 2002). Kahneman, Knetsch and Thaler (1991) performed a comprehensive study to examine this WTA-WTP disparity. In their well-known experiment, the researchers offered randomly chosen students a coffee mug that could also be acquired at the university bookstore for $6.

The students were asked to examine a mug, either their own or the mug of one of their fellow participants. Then, the subjects were divided in two different groups: one group with the property rights to the good, which they could sell, and the other group without the property rights but able to bid for the coffee-mugs. The median WTP was $2.25 while the median WTA was $5.25. The number of trades that occurred was minimal due to the difference between WTA and WTP. Kahneman et al. (1991, p. 196) reported that: “despite the fact that the experiment was replicated several times, median selling prices were about twice median buying prices”. As a consequence, trade volumes were less than half of that expected. This phenomenon (the fact that people often demand much more to give up a good than they would be willing to pay to acquire it) labeled as the endowment effect (Knetsch and Sinden, 1984; Kahneman et al., 1991; Thaler, 1980).

Acquisti, John and Loewenstein (2013) tested the influence of the endowment effect on the valuation of information privacy. In their field experiment, the researchers offered free gift cards to a diverse group of shoppers in a shopping mall. Half of the participants were offered a $10 anonymous gift card whilst the remaining participants received a $12 card. However, this more valuable gifs card was mandatory to be linked to the personal information of the participants. Hence, the products acquired with the gift card were linked to the personal identity of the participant. After handing out the gifs cards, the participants had the opportunity to switch. Shoppers that possess the $10 gift card, were given the opportunity to require the $2 extra value in exchange for revealing their personal information. Contrary, the other respondents were able to switch to the less valuable card that ensures an anonymous shopping experience. The participants who originally held the $10 card held it five times as many compared to the persons originally held the $12 card. This result indicates that individuals value privacy at a higher level when they possess it (and thus are aware of it) compared to when they do not. In addition to Acquisti et al. (2013), Kehr et al. (2015) investigated the dynamics of the endowment effect on behavioral attentions as well. Both studies stressed that the psychological ownership of information privacy is one of the causes that provokes the inconsistency between stated privacy concerns and intended or actual privacy related behavior.

Kahneman et al. (1991) accentuated that the pain of giving up the good that one owns is the main cause of the endowment effect. In an earlier article Kahneman and Tversky (1979) referred to this phenomenon as loss aversion: “A salient characteristic of attitudes to changes in welfare is that losses loom larger than gains. The aggravation that one experiences in losing a sum of money appears to be greater than the pleasure associated with gaining the same amount” (Kahneman & Tversky, 1979 p. 279).

3 Research Design

In this section, the research design of the study is discussed. First, the research question will be recited and hypotheses are formulated. In addition, a brief summary of the theoretical framework that endorses the proposed hypotheses is given. The experiment, its constructs, variables and overall procedure are discussed in the second part of this chapter. A few modifications to the original data set were required to make the data applicable for the study. These adjustments are discussed and the descriptive statistics of the altered data set are given. In the final part of this chapter, the assumptions for the analyses are discussed.

3.1 Research question and hypotheses

The main objective of the research is to study how framing effects can influence the intended behavior of consumers to reveal personal information. Hence, the proposed research question is:

How can framing effects influence consumers' willingness to disclose personal information in an e-commerce environment?

To develop a systematic and adequate answer to this inquiry, hypotheses need to be formulated motivated by a consolidation of the literature review. First of all, it is emphasized that information privacy related choices are not as stable or consistent as the privacy calculus assumes. Earlier studies have indicated that consumers often exhibit inconsistent behavior and that their stated privacy concerns are not explanatory for their actual or intended privacy related behavior. This dichotomy is termed the privacy paradox. A justification of the privacy paradox can be found in behavioral economic principles, that stresses that people are often biased, make inconsistent choices and rely on heuristics, or mental shortcuts, to simplify the complex decision that they have to make. For instance, the optimistic bias and wishful thinking could influence privacy related choices and thus causes inconsistency. Individuals underestimate their chances of becoming a victim of the opportunistic behavior of online vendors and judge themselves to be less vulnerable to the risks of revealing the personal information compared to others. A consequence of this contradictory behavior is that the privacy related choices of consumers could be guided by non-normative factors. An example of such non-normative factors are framing effect, indicating that choices can be presented in a matter that highlights certain aspects of a decision and thus appeal differently to the actor.

In addition, a significant amount of research has accentuated on the benefits of the personalization strategy for online consumers. Personalization enhances several customer benefits as convenience and individualization. Contrary, the risks of revealing personal information are enhanced by the overoptimistic behavior of online vendors. Online vendors might sell the personal information to third party companies or utilize private data for price discriminations.

An evaluation of above provokes the question if priming the positive or negative consequences of revealing the personal information could influence the privacy related behavior of consumers. By highlighting the positive consequences of revealing personal information in an online setting, consumers might be persuaded to disclose their private data. As elaborated on in the previous chapter, obtaining the personal information of consumers enhances several competitive advantages for online vendors. Contrary, it is interesting to examine the effect of accentuating the negative consequences, i.e. the risks of revealing personal information to e-commerce retailers. Earlier studies have emphasized that people are reluctant to read the privacy statements of online vendors. If priming the risks of revealing personal information can influence the choice of consumers to disclose privacy data, is this a revolutionary finding for policy makers. Hence, by obligating the use of framing effects, governments can protect the consumer from risky behavior.

Motivated by this brief elucidation the first two hypotheses are formulated:

- H1: Highlighting the advantages of revealing personal information in an online environment enhances the willingness to accept of consumers.
- H2: Highlighting the disadvantages of revealing personal information in an online environment enhances the willingness to accept of consumers.

Furthermore, past research devoted to the valuation of information privacy accentuated the influence of the endowment effect. The endowment effect is a justification formulated by behavioral economists, for the WTA / WTP gap. This disparity refers to the difference between the average demand price for buyers and sellers for the same good. The willingness to accept of sellers is often much higher compared to the willingness to pay for buyers. The phenomenon is labeled as the endowment effect, which is an exemplification of loss aversion. It is interesting and pioneering to examine if the supposed inconsistency of privacy related behavior is caused by the endowment effect when individuals are primed. In both the positive as the negative priming, the information privacy awareness is increased and as a consequence, respondents can tend to evaluate their information privacy higher. Hence, respondents that are not primed can be more willing to reveal their personal information compared to the respondents that were either positive or negative primed. The second two hypotheses examine the presence of the WTA / WTP disparity and the endowment effect.

- H3: The willingness to accept is higher for the consumers that are either positively or negatively primed compared to the willingness to accept of consumers that are not primed.
- H4: The general willingness to accept is higher compared to the general willingness to pay of consumers.

The first three hypotheses constitute the main center of attention of the investigation and an extensive research of these inquiries is required to formulate an adequate answer to the research question. Nevertheless, this research assumes the legitimacy of the privacy paradox, an ambiguity that accentuates the dichotomy between the stated privacy attitudes of consumers and their actual or intended behavior. In other words, the online consumer exhibits inconsistent behavior. In accordance with behavioral economic theories, this type of behavior could be influenced by non-normative factors such as framing effects. As the research heavenly relies

on the privacy paradox, an additional hypothesis is formulated, that investigates the assumed dichotomy between stated privacy concerns and general willingness to accept. In addition, this hypothesis is pioneering in the research devoted to information privacy as it measures the privacy concerns of consumers on a continuous scale. Earlier research have categorized their respondents into three different privacy profiles and concluded based on these categorical variables.

- H5: The privacy concern of consumers is not explanatory for the general willingness to accept of consumers.

To ensure that the three main hypotheses are explanatory and comprehensive, several sub-hypotheses are formulated. These sub-premises test among for correlations between the framing effects and the privacy concerns of individuals. An overview of all hypotheses and results can be found in Appendix 1.

3.2 The experiment

An online questionnaire was developed utilizing the web software "Qualtrics". The survey was distributed trough the personal Facebook page of the author. Through clicking on a link that was promoted on the "wall" of the Facebook page, respondents could access the questionnaire. By only distributing the questionnaire through Facebook, a relatively homogenous sample can be reached. Most Facebook friends of the author are highly educated young professionals that are expected to frequently shop online. Furthermore, there was no incentive provided to participate in the experiment due to budget constraints. An outline of the questionnaire can be found in Appendix 2.

The main objective of the experiment is to identify the causal inferences between the framing effects and the willingness to share personal information. The causal inference can be indicated when the behavior in identical situations is compared but when one variable is manipulated. Hence, two different framings effects along with a baseline effect are included in the research. The respondents were randomly assigned to the three treatment conditions and subsequently asked to reveal their willingness to accept based on the particular priming. Figure 1 illustrates a detailed overview of the experimental design. The variables of interest are illustrated in the squared boxes whilst the framing effects are indicated in the ovals.

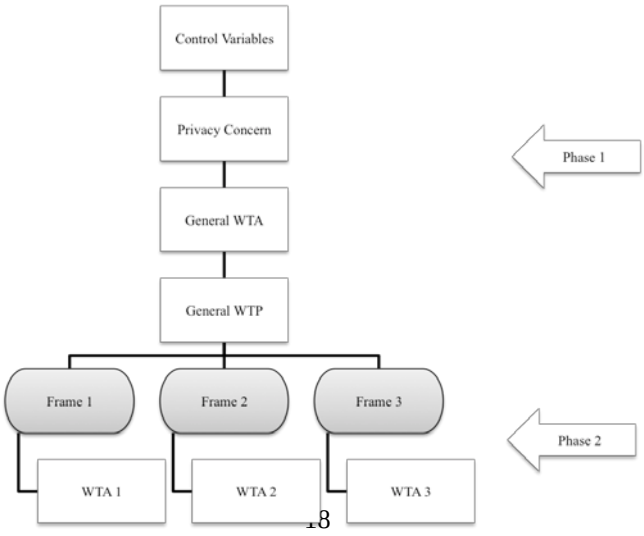


Figure 1: Schematic overview of experimental design

3.3 Phase 1 of the experiment

3.3.1 Control variables

The experiment consists of two different phases. As illustrated by the overview of the experimental design (figure 1), the first phase is identical for all respondents. After reading a short introduction, all respondents are asked to fill in some demographic characteristics. As elaborated in the theoretical framework, the willingness of consumers to reveal personal information is affected by demographics (e.g. Xu et al., 2008; Cho et al., 2009; Sheenan, 1999). Nevertheless, the aim of this research is to examine the influence of framing effects. Hence, the demographics function as a control variable to ensure that the respondents are randomly assigned to the different treatments in the second part of the questionnaire. The model includes four control variables: age, gender, frequency of online shopping and highest level of completed education.

3.3.2 Privacy concern

In the second part of the first phase of the questionnaire, respondents are asked to answer online privacy related questions by filling in a 7-point Likert-scale. The privacy concern questions are originally formulated by Westin (1991) but adjusted by Jensen et al. (2005) in the context of e-commerce. The five questions as formulated by Jensen et al. (2005) are adopted. Nevertheless, earlier studies that examined the privacy concerns of consumers used the measure to categorize their respondents into the Westin privacy segmentation (Jensen et al., 2005; Spiekermann et al., 2001). This index divides the respondents into three different segments: fundamentalist, pragmatist and unconcerned (Jensen et al., 2005; Spiekermann et al., 2001). Subjects that gave privacy-oriented answers to all questions are classified as fundamentalist, whilst those that gave no privacy oriented answers were labeled as unconcerned. Participants that answered in-between were identified to be pragmatists. This study differs from previous research as the privacy concern of the respondents is measured on a 7-point Likert-scale. This Likert-scale ranges from 1 (strongly agree) to 7 (strongly disagree). Consequently, a lower score indicates more care for privacy and the differences in the scores demonstrates the people different degrees in privacy concerns. The following five statements are valued on the 7-point Likert-scale:

Table 1 – Overview of questions measuring privacy concern

Q1	I am concerned about my privacy in everyday life.
Q2	I am concerned about privacy theft.
Q3	I am concerned about my privacy online.
Q4	I am likely to read the privacy policy of an e-commerce website before buying anything.
Q5	Privacy policies accurately reflect what companies do.

3.3.3 General Willingness to Accept and General Willingness to Pay

The general willingness to accept (GWTA) is a construct that measures the discount that respondents wish to receive in exchange for revealing personal information. A high level of general willingness to accept indicates that the respondent has a low willingness to reveal personal information. After all, the participant values his personal information as precious and is not willing to reveal the private data in exchange for a small financial incentive. Likewise, a high level of general willingness to pay expresses a high valuation of the personal information and thus a low level of willingness to disclose the personal data.

As elaborated on in the theoretical framework, earlier research has accentuated on the WTA / WTP gap (e.g. Kahneman et al., 1991). Different from what is assumed by standard economic theories is there a disparity between WTA and WTP. Horowitz and Kenneth (2002) reviewed 45 studies that observed this WTA / WTP dichotomy and summed the different research techniques utilized to measure the inconsistency. The scholars examined three main techniques that are used to measure the WTA and WTP:

1. A direct open-ended question such as "*What is the maximum amount you are willing to pay to obtain good X?*"
2. An open-ended question that is compatible with an incentive as Vickery auctions or the Becker-deGroot-Marschak mechanism.
3. A closed ended question. Responds are asked to select the value that reflects their WTA or WTP.

This study adopts the third technique and asks the respondents to select their WTA and WTP after reading a short introduction. The motivation for not choosing the second option is that there is no budget to reward the respondents with an incentive. Furthermore, people might be unfamiliar with evaluating their information privacy (Awad & Krishnan 2006). Hence, by adopting the first method, divergent extremes values can be found. In addition, these extremes can negatively impact the power of the analysis. Therefore it is chosen to adopt the third technique.

The question that examines the WTA stresses that online vendors are offering their consumers small discounts in exchange for revealing some personal information. The respondent is asked to select the value that reflects the discount they are willing to receive in exchange for revealing: full name, e-mail address, age and gender. The general willingness to accept is therefore measured by the following question:

Table 2 - Question that examines the general willingness to accept of consumers.

These days, some online retailers are offering their (potential) customers a small discount in exchange for disclosing personal information. How much discount should an online-retailer offer you to reveal your: full-name, e-mail address, age and gender?

- o I do not require a compensation to reveal my personal information. (1)
- o 0 - € 2.50 (2)
- o € 2.50 - € 5 (3)
- o € 5 - € 7.50 (4)
- o € 7.50 - € 10 (5)
- o More than € 10 (6)
- o I am not willing to reveal my personal information for any given discount. (7)

Contrary to the general willingness to accept, the general willingness to pay examines the amount that consumers are willing to pay to protect their privacy. These days, there are different services that customers can acquire to prevent disclosure of personal information. As an example, consider the many anonymous Web-browsing applications as Tor and the option to disable third-party cookies in popular browsers as Firefox and Google Crome (Acquisti et al., 2013). Hypothetically, an anonymous shopping experience can be ensured by a service that offers customers the possibility to conceal their personal information behind an anonymous number. If a consumer decides to purchase a product from an online vendor, the customer only has to disclose his personalized number to complete the purchase. The service company safely holds the personal information and enables the delivery and payment transaction. In addition, the company has no incentive to abuse the personal data as customers pay a fee in exchange for upstanding behavior.

To my best knowledge, there are no companies offering this type of service. However, for the purpose of the research, the following hypothetical question that emphasizes on such a services is formulated:

Table 3 - Question that examines the general willingness to pay of consumers.

Many online retailers use your personal information for divergent purposes, e.g. price discrimination, marketing purposes or sell your data to third parties. Suppose you are given the opportunity to ensure an anonymous shopping experience by utilizing a pseudonym in the form of a number. Hence, you are not obliged to reveal any personal information such as: full-name, e-mail address, age nor gender to the online-retailer. How much are you willing to pay for this one time service?

- ❍ I am not willing to pay any commission for this type of service. (1)
- ❍ 0 - € 2.50 (2)
- ❍ € 2.50 - € 5 (3)
- ❍ € 5 - € 7.50 (4)
- ❍ € 7.50 - €10 (5)
- ❍ More than € 10 (6)

Furthermore, earlier studies have emphasized that people value various types of personal information differently. For instance, Huberman, Adar and Fine (2005) researched the WTA of revealing body weight and height. This amount was significantly higher than the WTA for disclosing the participants' home address. To ensure that this study is realistic and thus in consequent with real online-shopping scenarios, the respondents are asked to value their personal information consisting of full name, e-mail address, age and gender.

The stated values of general willingness to pay and general willingness to accept are small amounts from a few euros. Although some earlier studies have measured extreme valuations of WTA and WTP of information privacy, most researchers agree that both the willingness to accept and the willingness to pay should be small. This is also consistent with the actual discounts that online vendors are offering on their websites and the costs of browsers that enable an anonymous shopping experience (Awad & Krishnan, 2006).

The four different elements of the first phase (i.e. demographics, privacy concern, WTA and WTP) of the experiment are randomized to exclude undesired ordering effects. The randomization strategy is illustrated by the survey outflow in Appendix 3.

3.4 Phase 2 of the experiment

3.4.1 The framing effects and the post-priming willingness to accept

In the second part of the questionnaire respondents, are shown one of the three different pop-ups that appears while shopping for headphones at a well-known online webstore. The outlooks of the pop-ups are manipulated with either a positive, negative or neutral framing effect. The positive framing effect emphasizes the possible advantages revealing personal information, i.e. the option for personalized offers and services. Contemporary studies accentuated that the option for personalized services is one of the biggest advantages of disclosing private data (Awad & Krishnan, 2006; Lee & Cranage, 2011; Tam & Ho, 2005). Contrary, the second framing effect accentuates the possible risks of revealing personal information online. Earlier research has accentuated that the major risk factor that enhance privacy concerns is the opportunistic behavior of online vendors including selling personal information to third parties, unauthorized access and fraud (Dinev & Hart, 2006). The third framing effect is neutral and functions as the base category.

After the respondents are either positively, negatively or neutral primed by being disclosed to the framing effects, their willingness to disclose personal information is once again questioned. As in the first part of the experiment, this willingness to reveal the personal information is measured as a general willingness to accept. Hence, a higher level of willingness to accept indicates a lower willingness to disclose personal information due to the fact that the respondents value the personal information as more precious. This willingness to accept is labeled as the post-priming willingness to accept and is measured for the three conditions. Table 4 illustrates an overview of the utilized framing effects and the corresponding reaction of the respondents.

Table 4 – Overview of framing effects

Frame	**Highlights**	**Post-priming WTA**
Frame 1 – Positive	Benefits - Personalization strategy	WTA1
Frame 2 – Negative	Costs - Opportunistic behavior of online vendors	WTA2
Frame 3 - Neutral	Not applicable	WTA3

The outlook of the website is inspired an original pop-up on the webstore of the jeans brand “Seven for all Mankind”. The privacy statements of Google served as a model for the content of the negative framing. A copy of this original pop-up and the content of Google can be found in Appendix 4. The outlooks of the framing effects are presented in Appendix 5.

3.5 List of variables

Table 5 constitutes an overview of the variables employed to test the formulated hypotheses. Some variables are not directly questioned in the survey but generated out of the original constructs. Elucidations on these new variables are given in the subsequent paragraphs whilst table 6 provides an overview.

Table 5 – Overview of Variables employed

Type	Variable	Abbreviation	Type
Control variable	Gender	GEN	Nominal
	Age	AG	Ordinal
	Highest level of completed education	EDU	Ordinal
	Frequency of shopping online	Freq_On_purc	Ordinal
Variable	General willingness to accept to give up personal information	GWTA	Ordinal
	General willingness to accept to protect personal information	GWTP	Ordinal
	Willingness to accept after being primed with the positive frame.	WTA1	Ordinal
	Willingness to accept after being primed with the negative frame.	WTA2	Ordinal
	Willingness to accept after being primed with the neutral frame.	WTA3	Ordinal

Table 6 – Overview of generated variables

Variable	Meaning	Method	Scale
Delta_WTA	Difference between general willingness to accept and post priming willingness to accept	GWTA – Post_WTA	Ordinal
Privacy_Concern	Privacy concern	Average of answer to Q1 – Q4 (7-point Likert-Scale)	Interval
WTA_WTP	WTA / WTP gap	GWTA - WTP	Ordinal
Post_WTA	Willingness to accept after being primed	WTA1 + WTA2 + WTA3	Ordinal
Condition	Priming	1 = positive 2 = negative 3 = neutral	Nominal

3.5.1 *The difference in WTA*

In order to accurately measure the difference between the general willingness to accept of respondents and the post framing willingness to accept, a new variable is created. This variable is the Delta_WTA and measures the difference between a respondent' GWTA and post-priming WTA. By creating this new variable, it can be ensured that the GWTA corresponds to the post WTA and unwanted effects are eliminated. Hence, this new variable can measure the impact of different framing.

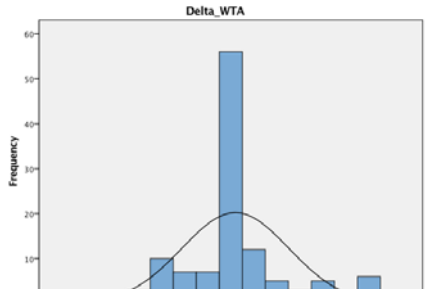


Figure 2: Histogram frequency count difference in WTA

3.5.2 *The privacy concern measurement*

The construct of privacy concern is measured by 5 different questions enlisted from the research of Jensen et al. (2005). Nevertheless, to ensure that these questions are explanatory for the level of privacy concern, the Cronbach's Alpha needs to be computed. The Cronbach's Alpha for the five questions is 0,567 and thus insufficient. An examination of the correlations between the questions emphasized that question 5 is the weakest question. This is consistent with the expectations as this question examines the accuracy of privacy related policies and has little equivalence with the privacy concerns of individuals. Therefore, question 5 is not included in the privacy concern measure, which now has a sufficient Cronbach's Alpha of 0,738. The respondents answered the 4 privacy related questions on a 7-point Likert-scale. In this Likert-scale, 1 is strongly agree, whilst 7 is strongly disagree. Therefore, the lower the Likert-scale score, the higher the levels of privacy concern. Furthermore, the privacy concern measure is then the average score of respondents on these 4 questions. This mean privacy concern is 3,73 with a standard deviation of 1.17. A histogram of the scores in privacy concern illustrates a normal distribution as demonstrated by figure 3. The mean privacy concern is 3,73 with a standard deviation of 1,17. (For the statistical output of the analysis, see Appendix 6).

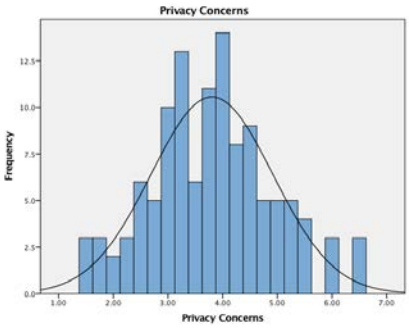


Figure 3: Histogram frequency count Privacy Concern

3.5.3 *The WTA / WTP gap*

The disparity between the willingness to accept and willingness to pay is measured by a new variable: the WTA / WTP gap. This variable is conducted by subtracting the general willingness to pay from the general willingness to accept. The mean WTA / WTP gap is 2.23 with a standard deviation of 2.174. The median is 2.00 and the WTA/WTP gap minimum value is -3 whilst the maximum 6. See also figure 4.

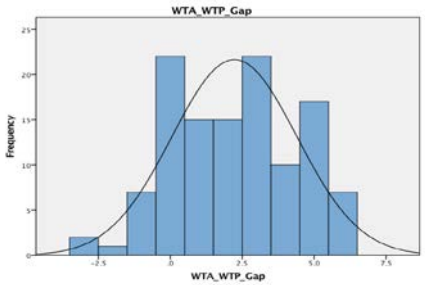


Figure 4: Histogram frequency count WTA / WTP gap

3.6 Assumptions

As stated in the variable overview table, the scale of measurement of most variables is measured at a Likert-scale. Likert-scales are a group of categories (ranging from least to most) asking people how much they agree or disagree with a given statement. There is a lot of controversy in the literature on data analysis whether the Likert-scale needs to be considered as interval or ordinal data (Allen, Seanman, 2007). The first scale of measurement refers to a type of data in which ordering and distance measures are possible, for instance the weight of respondents (McCrum-Gardner, 2008). The ordinal level on the other hand denotes data in which ranking is possible but no measure of distance. An example of ordinal scale is the measurement of pain level, which could be mild/moderate/high (McCrum-Gardner, 2008).

A motivation for analyzing a Likert-scale measurement on an interval scale is that (normal distributed) interval data allows for parametric tests. Parametric tests are, compared to the non-parametric alternatives, more powerful. In addition, interpretations and conclusions of parametric tests are considered to be more transparent and informative (Allen & Seanman, 2007). Nevertheless, the original paper on the Likert-scale measurement stresses that there might be an underlying continuous variable that explains the choices of the consumers (Likert, 1932). This continuous variable is interval at best (Allen & Seanman, 2007). In addition, contemporary research accentuates that Likert-scales can be interpreted on an interval scale, as there is a sufficient Cronbach's alpha and the other assumptions are met (Boone & Boone, 2012). As the Cronbach's alpha of the privacy concern is sufficient, it is decided to analyze the construct at an interval scale.

The other variables, the general willingness to accept, post priming willingness to accept and willingness to pay are measured at the ordinal scale: there is at least an ordering of responses possible. The respondent is asked to choose the appropriate value ranging from "I do not require a compensation" to "I am not willing to reveal my personal information for any given discount." The data scales between these extremes value vary with € 2.50. Just as the advocates of the interval interpretation of Likert-scale data, there are many studies that emphasize the correctness of measuring ordinal data with analysis that are suitable for interval measurements (e.g. ANOVA, T-test) (Allen & Seanman, 2007; Boone & Boone, 2012). The main argument is that the "the interverallness is an attribute of the data, not the labels" (Allen & Seanman, 2007 p. 65). This is often the case when the ordinal scale refers to monetary values. This argument is suitable for the scale utilized to measure the general willingness to accept, post priming willingness to accept and general willingness to pay as well. The scales vary with equal steps of €2,50 and it is questionable how the respondents value the "more than €10" option. It is theorized that if equal (monetary) scales are utilized, the extreme scales are valued in line with this measure (Allen & Seanman, 2007). Therefore, the extreme value "more than €10" can be comprehended as € 12.50 and this transformation allows for a measure distance. It is therefore decided to interpret the GWTA, WTP and post-priming WTA at first at the interval scale and employ the parametric tests.

Nevertheless, treading ordinal data as interval data without examining the values of the dataset and the objectives of the analysis can result in misinterpreting the data and stating wrong conclusions. Therefore, to ensure that the results are obtained correctly, non-parametric tests are employed as well.

3.7 Data preparation and data description

In total 157 respondents started the online questionnaire, although 31 respondents failed to complete the survey and are therefore deleted. Furthermore, 1 respondent emphasized that he had never shopped online. As the objective of this research is to study the willingness of consumers to reveal their personal information in an e-commerce context, this respondent is unrelated to the study and thus deleted from the data set. Therefore, there are in total 125 respondents that completely filled in the questionnaire and had made an online purchase in the past. Most respondents are between 25 and 34 (N=82) 18 and 24 (N=36) years old. There are no respondents younger than 18 (N=0) and only a few respondents are older than 34 (N=7).

The statistical power of a test can be improved by having a homogeneous sample. Therefore, it is debatable to exclude the 7 respondents that are older than 34. The sample then becomes homogenous and consists of highly educated adolescents varying from 18 to 34 years old, which made an online purchase in the past. To support this decision, the independency of the descriptive variables is examined by utilizing a chi-square test. This analysis shows that all the variables are independent, except for age and frequency. Older people (age > 34) shop less often online compared to younger people (age ≤ 34). Nevertheless, there are not enough old respondents to draw statistically valid conclusions for old people (N =7). In addition, earlier studies have already accentuated that older people shop less frequently online compared to adolescents. In addition, the relationship between the control variables (i.e. education, age, gender and frequency online purchases) and the continuous variables (GWTA, GWTP, WTA, PC) are preliminary tested by utilizing a one-way ANOVA analysis. Gender, frequency purchase and education have no significant influence on any of the continuous variables. Only age (categorized in old (age > 34) and young (age ≤ 34)) has a significant influence on GWTA ($p = .004$) and PC ($p = .006$). Hence, to improve the statistical power of the test, it is decided to eliminate the 7 participants that are older than 34 from the data set as well.

After adjusting the data there are total of 118 independent observations at the individual level. More females (N=74) compared to males (N=44) completed the survey. In addition, most respondents are between 25 and 34 years old (N=82) and highly educated as most participants received a Master's degree (N=54) or even a PhD (N=1). Only a few participants (N=14) possess just a high school degree but chances are high that these respondents are still students. The mean general willingness to accept is 4,36 whilst the mean general willingness to pay is 2,03. The mean willingness to accept post priming is 4,50. However, these means are trivial as the data is originally measured on ordinal scales. Hence, the median general willingness to accept is 4.00 and the median general willingness to pay is 2.00. The median willingness to accept post priming is 5. The distributions of the control variables are presented below. For an extensive description of the data, see Appendix 7 and 8.

3.7.1 Randomization of the treatments

It is highly important that the respondents are randomly assigned to the three different treatments. By examining the distribution of the control variables among the treatments, this randomization can be tested and ensured. In total 38 respondents were exposed to the positive treatment (framing 1, N = 38), 39 respondents to the negative treatment (framing 2, N = 39) and 41 to the neutral treatment (framing 3, N = 41). By utilizing a Chi-square analysis it can be tested if the sample is equally distributed over the three different treatments (positive framing, negative framing and neutral framing). The data meets the two assumptions for the Chi-square tests, i.e. the variables are ordinal or nominal and there are more than two independent groups. The randomization is successful as there is no significant association between the control variables and the treatments. In Appendix 7 an extensive description of the statistical test results is given.

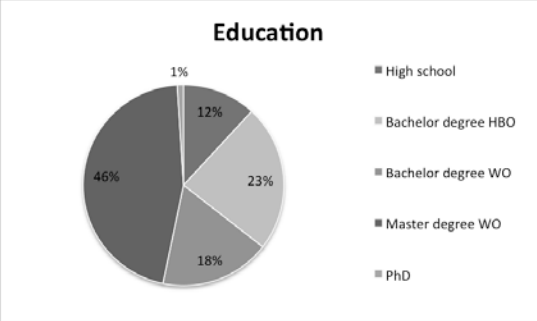


Figure 6: Distribution of education.

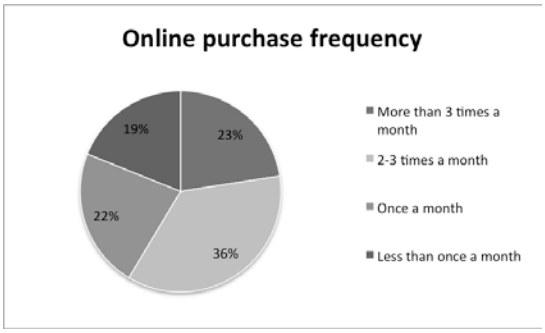


Figure 7: Distribution of online purchase frequency.

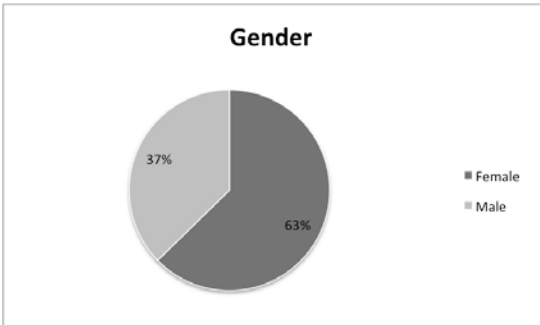


Figure 8: Distribution of gender.

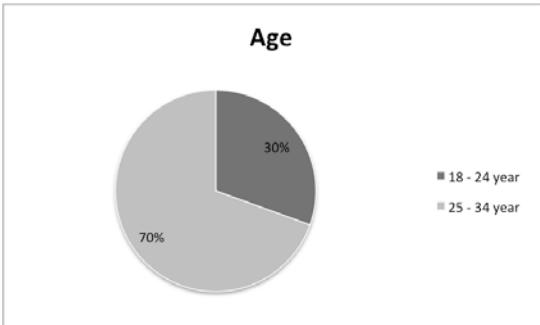


Figure 9: Distribution of age.

3.7.2 Including contrast coefficients

The aim of the study is to test the difference between the WTA of the framing effects. To examine the hypothesized difference contrast coefficients are created. These coefficients enable a comparison between the mean of population and is more specific than a general One-way ANOVA analysis as it provides a more detailed understanding. If there are more than 2 treatments, including contrast coefficients provides exact insights in the difference between treatments (Janssens et al., 2008). As this study examines three different treatments, contrasts coefficients are included. First, the difference between the positive or negative treatment and the neutral treatment are hypothesized.

$$H_1 : \mu_{positive} \neq \mu_{neutral} \quad (1)$$

$$H_2 : \mu_{negative} \neq \mu_{neutral} \quad (2)$$

In addition, the difference between the combined average mean of the positive and negative treatments are compared to the neutral framing effect. A significant difference between these means can be the result of the endowment effect. Hence, both the positive as the negative treatment accentuates the privacy of the respondent. In line with the theory of the endowment effect as elaborated on in the previous section, this could mean that people value their personal information higher compared to the neutral treatment in which there is no emphasize on information privacy. Therefore a third complex contrast hypothesis is formulated.

$$H_3 : \frac{\mu_{positive} + \mu_{negative}}{2} \neq \mu_{neutral} \quad (3)$$

A contrast coefficient table (see table 7) is conducted in SPSS and is utilized in the One-way ANOVA analysis.

Table 7 - Contrast Coefficients

	Condition		
Contrast	Positive	Negative	Neutral
1	1	0	-1
2	0	1	-1
3	1	1	-2

3.7.3 Correlation analysis

A correlation analysis has been performed for the continuous variables to gain a general overview of the data (see table 7). The analysis identifies a significant correlation between "General Willingness-to-accept" (GWTA) and post treatment "Willingness-to-Accept" (WTA). This relationship points out that the GWTA of the respondents is explanatory for the WTA. This correlation is obvious, although the framing effects are assumed to influence to the post-priming WTA of the respondents, they are unlikely to completely change the attitude of the respondents

Furthermore, the level of privacy concerns (PC) of individuals is negatively related to GWTA. The privacy concern is the average answer on a 7-point Likert-scale to four privacy concern related questions. A low privacy concern score indicates a high level of actual privacy concern. Therefore, this negative correlation illustrates that the lower the actual level of privacy concerns, the lower the general willingness to accept. Subsequently, high privacy concerned consumers are reported a high willingness to accept and are therefore less willing to disclose their personal information. This correlation negates the privacy paradox and is an interesting (preliminary) finding. The privacy paradox stresses that the levels of privacy concerns of consumers are not explanatory for their intended privacy related behavior. Hence, people that reported high levels of (actual) privacy concerns tend exhibit a high willingness to disclose their personal information. Nevertheless, additional analyses are required to correctly formulate conclusions.

Furthermore, the correlation matrix (table 8) illustrates a significant negative correlation between privacy concern and the willingness to pay of consumers. This relation emphasizes that the higher the actual privacy concerns of consumers (and thus the lower the privacy concern measure) the more willing to pay to protect their online privacy. This finding contradicts the main premises of the privacy paradox as well but is nevertheless consistent with the reported negative relationship between privacy concern and general willingness to accept of the analysis.

Finally, the correlations between the variables and the difference between general willingness to accept and post priming willingness to accept are examined. This variable is conducted by subtracting the post WTA from GWTA. Therefore, it is not surprising to find that the Delta_WTA and GWTA are negatively correlated. Similar, the Delta_WTA is positively correlated to the post-priming WTA variable.

Table 8 - Correlation Matrix of Variables.

	Mean	Std. D.	Chron. α	1.	2.	3.	4.	5.
1. GWTA	4,24	1,97	-	1				
2. WTP	2,01	1,95	-	0,126	1			
3. Post WTA	4,43	2,02	-	0,321**	- 0,037	1		
4. PC	3,80	1,16	0,738	- 0,293**	- 0,199 *	- 0,103	1	
5. Delta_WTA	0,1949	2,33	-	- 0,568**	- 0,139	0,597**	0,159	1

*** Correlation is significant at the 0,01 level (2-tailed).*

** Correlation is significant at the 0,005 level (2-tailed).*

4 Results

In this part of the thesis the results on the formulated hypotheses will be presented. First the influence of the framing effects is tested and thus hypotheses 1 – 3 are examined. If the framing effects are effective, there should be a significant difference between the three different "post willingness to accept". Consequently, the value of "delta willingness to accept" should be significantly different than 0. An additional analysis is conducted to test the influence of the priming effects on this delta willingness to accept.

After concluding on the three main hypotheses, the proposed difference between the WTA and WTP is investigated. Difference between willingness to accept and willingness to pay accentuates the inconsistency in privacy related behavior. Furthermore, this dichotomy could be a caused by the endowment effect. Finally, the fifth hypothesis that scrutinizes the relationship between privacy concerns and willingness to accept is tested. This hypothesis examines the validity of the privacy paradox.

4.1 Hypotheses 1 – 3: The impact of framing effects on the willingness to accept.

The first three hypotheses examine the impact of the framing effects on the willingness to accept of consumers. After being either positive, negative or neutral primed, the survey asks respondents to select the amount of discount that they are willing to accept in exchange for revealing: full-name, e-mail address, age and gender. Hence, the three post priming willingness to accept could be compared. Furthermore, a higher level of willingness to accept indicates that the consumer is less willing to disclose personal information.
Four analyses are conducted to make this comparison in an applicable manner. First three different parametric tests are conduct (One-way ANOVA and One-sample T-test). Thereafter an additional non-parametric test (Kruskal Wallis) is employed. These four analyses and their results are discussed before a conclusion on the first three hypotheses is formulated.

4.1.1 Analysis 1 - The influence of the framing effect on the respondents' willingness to accept.

The main hypotheses question the difference between the post priming WTA of respectively the positive and negative frame compared to the baseline effect (i.e. the neutral framing). If the framing effects influence the willingness of consumers to reveal their personal information, a difference in post priming WTA should be detected. The hypothesis of this test is formulated as follows:

$H_0 =$ The post priming willingness to accept for the conditions are equal.

$$H_0: WTA_1 = WTA_2 = WTA_3 \quad (4)$$

$H_1 =$ At least one of the post-priming willingness to accept for the conditions is not equal.

$$H_1: NOT: WTA_1 = WTA_2 = WTA_3 \quad (5)$$

To examine these dissimilarities, contrasts coefficients are formulated (see table 6 on page 30). The impact is measured on the post priming willingness to accept, i.e. the dependent variable. As discussed in the previous chapter, the willingness to accept is measured at an ordinal scale but interpreted as an interval variable. Hence, One-Way ANOVA analysis can be employed to examine the difference between the post-priming willingness to accept of consumers. As accentuated, there is interdependence of observations for the three framing effects. A second assumption of a One-Way ANOVA analysis is that there is homogeneity of variances. This is tested by a Levene's test for equality of variances. The null hypothesis states that the population variances are equal. This test indicates that the variances in post WTA are not significantly different for the three conditions: F (2, 115) = .378, p = .686. Therefore, equal variances can be assumed. Subsequently, a One-way ANOVA analysis shows that the mean post WTA is not significantly different between the three framing effect: F (2, 115) = .312, p = .773. In addition, the contrast tests results (see table 9) indicates that there are no significant difference between the formulated contrasts on the post willingness to accept.

Table 9 – Contrast test

1	Positive framing – Neutral Framing	t (115) = - .637	p = 0.525
2	Negative framing – Neutral Framing	t (115) = - .717	p = 0.475
3	Not neutral framing – Neutral framing	t (115) = - .786	p = 0.434

Dependent variable: Post willingness to accept

This result indicates that none of the framing effects influence the post priming willingness to accept and thus the willingness to reveal personal information. (For statistical details, see Appendix 10.)

4.1.2 Analysis 2 - The difference between the general willingness to accept and the post willingness to accept.

As elaborated on the previous part of this thesis, a new variable is created to measure the strength of framing effects. By subtracting the post-priming WTA from the GWTA, delta WTA is created. If the framing effects influence the willingness to accept of consumers, this variable needs to be significantly different than 0.

$$H_0 = \text{Delta WTA is equal to 0.}$$
$$H_0\text{: Delta WTA} = 0 \quad (6)$$

$$H_1 = \text{Delta WTA is not equal to 0.}$$
$$H_1\text{: Delta WTA} \neq 0 \quad (7)$$

To test this condition, a One-Sample test is conducted. This analysis indicates that the delta WTA is not significantly different than 0: t (119) = .909, p = 0.365. Hence, the three different framing have no impact on the post priming willingness to accept. (For statistical details, see Appendix 11).

4.1.3 Analysis 3 - The influence of the framing effects on difference willingness to accept.

To ensure that the analysis is comprehensive, an additional One-way ANOVA analysis is conducted that measures the influence of the framing effects on delta WTA and thus the difference between general willingness to accept and post-priming willingness to accept. Similar to the One-way ANOVA testing the post WTA, a test of homogeneity of variances is conducted. This test indicates that the variances in delta WTA are not significantly different for the three conditions: F (2, 115) = 1.715, p = .185. Hence, equal variances can be assumed. A One-way ANOVA analysis shows that, as expected, the delta WTA is not significantly different between the three framing effect: F (2, 115) = .390, p = .678. In addition, the contrast tests results (see table 10) indicates that there are no significant difference between the formulated contrasts. The framing effects fail to create a significant difference between general willingness to accept and post priming willingness to accept. (For statistical results, see Appendix 11).

Table 10 – Contrast test

1	Positive framing – Neutral Framing	t (115) = .153	p = 0.878
2	Negative framing – Neutral Framing	t (115) = - .835	p = 0.406
3	Not neutral framing – Neutral framing	t (115) = - .572	p = 0.568

Dependent variable: Delta_WTA

4.1.4 Analysis 4 – Non-parametric test: Kruskal Wallis test

As stated in the previous sections of this thesis is the use of the parametric One-way ANOVA analysis debatable for the acquired type of data. An assumption of parametric tests is that the data is measured at an interval scale. As the data shows many similarities with interval scale data, it is chosen to run parametric tests. Nevertheless, to ensure that the findings of the parametric tests are adequate and the data is not misinterpreted an additional non-parametric test is conducted: the Kruskal Wallis test. This test examines the relationship between more than two independent samples (Janssens et al., 2008) and is employed to test if the post-priming willingness to accept differs for the conditions.

$H_0 =$ The median of the post priming willingness to accept is equal among the three conditions.

$$H_0: \theta_1 = \theta_2 = \theta_3 \quad (4)$$

$H_1 =$ At least one of the medians of the post priming willingness to accept is not equal among the three conditions.

$$H_1: \text{NOT: } \theta_1 = \theta_2 = \theta_3 \quad (5)$$

The result of the Kruskal-Wallis test learns that there is no significance difference in median willingness to accept in each of the conditions: Chi-square (2) = .571, p = 0.752. Hence, the framing effects do not influence the willingness to reveal their personal information and this finding correspondent with the results of the parametric tests. (For statistical output see Appendix 13.)

4.1.5 Conclusion hypotheses 1-3

Taken these four analyses together, the results indicate that framing the consumer has no significant effect on their post priming willingness to accept. Hence, the willingness of consumers to reveal personal information in an online context cannot be influenced by framing effects. This conclusion is supported by the results of four analyses. First of all, a parametric One-way ANOVA indicated that the framing effects failed to cause a difference in post priming willingness to accept. Consequently, the post priming willingness to accept does not differentiate when the consumer are positive, negative or neutrally primed. Therefore, it could be questioned if there is a significant difference between general willingness to accept and post priming willingness to accept. A One-sample T-test accentuated that this disparity is not significantly different than 0 and does not exists. In other words, there is no significant difference between general willingness to accept and post priming willingness to accept and the framing effects lack any impact. This result is additionally supported by the third analysis that tested the influence of the framing effects on the difference between the general willingness to accept and the post priming willingness to accept. Once again, no significant results were founded. Finally, a non-parametric test was conducted to examine if the median of the three conditions differentiated. This analysis illustrated that the medians are equal among the priming effects. Therefore, the overall conclusion is that framing effects cannot enhance the willingness to accept of consumers and thus fail to influence the willingness of revealing personal information in an online environment.

Furthermore, it was hypothesized that difference between post-priming willingness to accept might be caused by the endowment effect. This effect could be measured by examining the third condition, i.e. the not neutral priming effect (both positive and negative) compared with the neutral priming effect. As elaborated on in the previous section, the comparison can measure the endowment effect as consumers that are primed have become more aware of their information privacy. Nevertheless, there is no significant difference measured in the third condition, meaning that the willingness to accept is equal among respondents that are primed and respondents that are not primed. Therefore, the endowment effect does not influence the willingness to reveal personal information of consumers.

Motivated by these findings all three hypotheses are rejected (see table 11).

Table 11 – Hypotheses 1, 2 and 3 & Conclusion

H1	Highlighting the advantages of revealing personal information in an online environment enhances the willingness to accept of consumers.	No
H2	Highlighting the disadvantages of revealing personal information in an online environment enhances the willingness to accept of consumers.	No
H3	The willingness to accept is higher for the consumers that are either positively or negatively primed compared to the willingness to accept of consumers that are not primed.	No

4.2 Hypothesis 4: The gap between willingness to accept and willingness to pay

The WTA / WTP gap is demonstrated by various studies and the willingness to accept is identified to be higher compared to the willingness to pay. Therefore, hypothesis 4 postulates that the general willingness to accept is higher compared to the general willingness to pay. In the realm of information privacy, this gap is considered to be relevant as it accentuates the inconsistency in privacy related behavior and that valuations of privacy are sensitive for non-normative influences.

4.2.1 Analysis 5: The WTA / WTP gap

First of all, subtracting the willingness to pay from the general willingness to accept creates a new variable: the WTA / WTP Gap. A frequency count of this new variable illustrates a normal distribution of the difference between the general willingness to accept and willingness to pay (figure 4, page 26). The mean of the gap is 2,23 with a standard deviation of 2,174. Nevertheless, to examine if the WTA / WTP gap is significant the following hypothesis needs to be examined:

$$H_0 = \text{The WTA / WTP gap is equal to zero.}$$
$$H_0: WTA/\text{ WTP gap} = 0. \quad (6)$$

$$H_1 = \text{The WTA / WTP gap is bigger than zero.}$$
$$H_1: WTA/\text{ WTP gap} > 0. \quad (7)$$

As the WTA / WTP gap seems to be normally distributed (see figure 10), a One-Sample T-test is conducted. This tests identifies that the WTA / WTP is significantly different than 0: $t(117) = 11.138$, $p = .001$. People tend to ask more to disclose their personal information compared to their willingness to pay to protect their personal information. Hence, hypothesis 4 is supported.

Earlier research has accentuated that this WTA / WTP gap can be caused by the endowment effect. However, the previous three analyses illustrated that there is no impact of the endowment effect in this experiment as the post priming willingness to accept is equal for all three conditions. Therefore, another explanation for the WTA / WTP gap should be given. Possible explanation will be discussed in the next chapter of this thesis.

Table 12 – Hypothese 4 & Conclusion

H4	The general willingness to accept is higher compared to the general willingness to pay of consumers.	Accepted

4.3 Hypothesis 5: The privacy paradox

The final hypothesis examines the privacy paradox by scrutinizing the relationship between the privacy concern and general willingness to accept. The privacy paradox postulates that the privacy concern of individuals is not explanatory for the actual or intended privacy related behavior. People that accentuated to be highly concerned about their online privacy still bargain their personal information for relatively small discounts.

4.3.1 Analysis 6: The relationship between privacy concerns and the general willingness to accept

Contrary to earlier studies, the privacy concern of individuals is in this research measured on a 7-point Likert-scale. The privacy concern variable is the average answer of the respondent to four privacy concern related questions, measured on this 7-point Likert-scale. In addition, a low privacy concern measure indicates (very) high level of privacy concerns. As the privacy concerns measures the average answer to four different questions that have a Cronbach's alpha > 0.70 the scrutinized relationship is allowed to be analyzed by a Simple OLS regression.

A simple linear regression analysis is employed to predict the general willingness to accept based on the privacy concern. A significant regression equation was found $F(1,116) = 10.916$ $p < 0.001$. The general willingness to accept of the participant will decrease 0.519 for each point of privacy concern. Hence, the level of privacy concern is explanatory for the general willingness to accept of respondents. The negative correlation identifies that the higher the privacy concern *measure* of the respondent, the lower the willingness to accept of the respondents. This results thus indicates that the lower the *actual* privacy concerns of the respondent, the lower the willingness to accept. Hence, the lower the *actual* privacy concerns of respondents, the more willing the respondent is to disclose its personal information. Subsequently, respondents with high *actual* levels of privacy concern, report a significantly higher level of willingness to accept and are therefore less willing to disclose their personal information. For any additional statistical output, see table 13, 14, 15 and Appendix 14.

Table 13 - Model Summary Linear Regression

Privacy Concern * GWTA

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
	.293a	.086	.078	1.894

a. Predictors: (Constant), Privacy Concerns

Table 14 – ANOVA (PC * GWTA)

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	39.164	1	39.164	10.916	.001b
	Residual	416.192	116	3.588		
	Total	455.356	117			

A. Dependent Variable: General Willingness To Accept

B. Predictors: (Constant), Privacy Concerns

Table 15 – Coefficients (PC * GWTA)

		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	t	Sig.
1	(Constant)	6.210	.622		9.982	.000
	Privacy Concerns	-.519	.157	-.293	-3.304	.001

a. Dependent Variable: General Willingness To Accept

4.3.2 Analysis 7: Non parametric test: Spearman's rho

For the same reasons as elaborated on earlier, a nonparametric test was conducted. The Spearman rank-order correlation is a measure that examines the association between two ordinal variables (Janssens et al., 2008). The analysis identified that there is a negative correlation between privacy concern and general willingness to accept, which was statistically significant Rs (116) = - .221, p = .016. See also table 16.

Table 16 – Non parametric correlations – Privacy Concern * GTWA

			Privacy Concerns	GWTA
Spearman's rho	Privacy Concerns	Correlation Coefficient	1.000	-.221*
		Sig. (2-tailed)	.	.016
		N	118	118
	GWTA	Correlation Coefficient	-.221*	1.000
		Sig. (2-tailed)	.016	.
		N	118	118

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

4.3.3 Conclusion hypothesis 5

The privacy paradox postulates that the stated privacy concerns of consumers are not explanatory for the intended or actual privacy related behavior of consumers. Hence, the privacy paradox stresses that people with high levels of privacy concerns exhibit the same disclosing habits as individuals that are inattentive to potential privacy violations. The lack of this correlation is scrutinized by the hypothesis 5.

Nevertheless, the results of the parametric regression, analysis 6, and non-parametric correlation analysis 7, identified that the levels of privacy concern is explanatory for the intended privacy related behavior of consumers: the level of privacy concerns are negatively correlated with the general willingness to pay. As elaborated in the previous chapter: a low privacy concern measure indicates high levels of actual privacy concerns. This rotation is due to the utilized 7-point Likert scale measurement that equals "strongly agree" to the value of 1 and "strongly disagree" to the value of 7. In addition, all questions examine the level of privacy concerns and are not reversed.

Hence, the results of the analyses indicate that people with a high level of actual privacy concerns have a higher willingness to accept. Therefore, these highly concerned individuals are less willing to disclose their personal information. Contrary to the main premise of the privacy paradox, is there a (negative) correlation between privacy concern and intended privacy related behaviors. Hypothesis 5 is therefore rejected.

Table 17 – Hypothese 5 & Conclusion

H5	The privacy concern of consumers is not explanatory for the general willingness to accept of consumers.	No

4.4 Conclusions regarding the formulated hypotheses

The main objective of the experiment was to investigate if the willingness of online consumers to reveal personal information could be influenced by utilizing framing effects. This inquiry emerged from an extensive examination of earlier studies on information privacy and the privacy paradox. This privacy paradox accentuates that individuals often exhibit inconsistent privacy related behavior. Consequently, the privacy related choices of consumers could be influenced by non-normative factors as framing effects. The first two hypotheses scrutinize the impact of positive and negative framing effects on the consumers' willingness to accept post priming. This dependent variable addresses the discount that the respondent wishes to receive in exchange for revealing: full-name, e-mail address, age and gender. Hence, the variable is correspondingly a measurement of the willingness to reveal personal information. The higher the willingness to accept of the respondent, the less willing (s)he is to reveal personal information.

By conducting contrast coefficients the difference between the willingness to accept of consumers that are positive, negative or neutrally primed could be compared. Nevertheless, there were no significant differences measured between the three conditions. Additional analyses were conducted to ensure that the founded equality was permissible and neither reported a significant difference. It is therefore concluded that the framing effects do not impact the willingness to accept of respondents. Hence, priming consumers with either the positive or negative consequences of revealing the private data, has no impact on the willingness of disclosing personal information in the form of: full-name, e-mail address, age and gender. As a consequence, the first two hypotheses are rejected.

The third hypothesis examines the effect of endowment on the willingness to disclose personal information. Priming consumers enhances their privacy awareness and it is therefore postulated that primed consumers value their information privacy higher compared to the consumers that are not primed. Hence, the willingness to reveal personal information will be lower for consumers that are primed. Nevertheless, as expounded no significant differences between the willingness to accept of consumers are measured. Therefore, it can be concluded that there is no impact of the endowment effect on the willingness to disclose personal information. Subsequently, the third hypothesis is also rejected.

Earlier studies have identified the endowment effect as a possible explanation of the WTA / WTP disparity. This dichotomy indicates that the willingness to accept of sellers is significantly higher compared to willingness to pay of buyers for the same good. The fourth hypothesis analyzed if this dichotomy is also pertinent when consumers appreciate their information privacy. Disunion of WTA and WTP confirms the premise of inconsistent behavior and as a consequence invalidates the popular privacy calculus. The analysis confirmed the existence of the WTA / WTP gap: the willingness to accept is significantly higher than the willingness to pay. Therefore the fourth hypothesis is accepted.

The final hypothesis investigates the fundamental privacy paradox that postulates that the privacy concerns of individuals are not decisive for privacy related behavior. However, the analyses identified that the privacy concerns is negatively correlated to the willingness to accept. In more detail, the results exemplify hat the higher the levels of the actual privacy concerns of the consumers, the higher their willingness to accept. Hence, the privacy fundamentalists are less willing to disclose their personal information compared to the privacy pragmatists. This is a direct contraction to the main premise of the privacy paradox that states that the

levels of privacy concerns are not explanatory for actual of intended privacy related behavior. Hence, the final hypothesis is rejected and with that the validity of the privacy paradox.

Table 18 – Overview of all hypotheses and conclusions

H1	Highlighting the advantages of revealing personal information in an online environment enhances the willingness to accept of consumers.	No
H2	Highlighting the disadvantages of revealing personal information in an online environment enhances the willingness to accept of consumers.	No
H3	The willingness to accept is higher for the consumers that are either positively of negatively primed compared to the willingness to accept of consumers that are not primed.	No
H4	The general willingness to accept is higher compared to the general willingness to pay of consumers.	Accepted
H5	The privacy concern of consumers is not explanatory for the general willingness to accept of consumers.	No

5 Discussion

This chapter summarizes the main findings of the research and composes a general conclusion. It is exemplified how these results relate but also differ to the general findings in the literature. Furthermore, the limitations of the design of the experiment are discussed. Based on these limitations, recommendations for future research are defined in the final part of this chapter.

5.1 General conclusion

Advances in technology and the tremendous success of e-commerce enhance information privacy concerns of consumers. Traditional research examining information privacy issues often utilized the privacy calculus. This model postulated that the decision of an individual to disclose personal information is the outcome of well-considered cost-benefit analysis. By carefully weighing the costs and benefits of disclosing, the decision-maker strategically chooses to share or not to share. Nevertheless, contemporary studies have demonstrated several flaws of the calculus and accentuated that people tend to make ambivalent privacy related choices. These researchers identified a common pattern of individuals that reported high levels of privacy concerns whilst simultaneously bargained their personal information for a dime. This ambiguity is examined in great extent and termed the privacy paradox.

The main premise of the privacy paradox thus postulates that individuals often exhibit inconsistent privacy related behavior. In addition, it is theorized that ambiguous behavior can be influenced by factors that are hard to explain on a normative base. For instance, choices can be framed by highlighting either the positive or negative aspects of a certain good, which impacts the decision of consumers. Inspired by the premise that people exhibit ambiguous privacy related behavior and the powerful impact of framing effects, the following research question was formulated:

"How can framing effects influence consumers' willingness to disclose personal information in an e-commerce environment?"

In addition, earlier parts of this report expounded that the inquiry is highly intriguing for policy makers and online vendors. The impact of the framing effects on the willingness to disclose personal information was then analyzed by utilizing an online questionnaire. Nevertheless, the results indicated that the framing effects failed to affect the behavior of the respondents. Therefore, the research question can be answered by stating that framing effects cannot influence the willingness to disclose personal information in an e-commerce environment.

Nevertheless, this conclusion begs the question *why* framing effects fail to influence the privacy related behavior of consumers and the second part of the study was devoted to this question. It was demonstrated that the levels of privacy concerns of respondents are decisive for the intended privacy related behavior. Or to be more precise, the results of the analysis identified that highly concerned individuals are less willing to disclose their personal information compared to individuals that are less concerned about their online privacy. This result is a direct contradiction to the main premise of the privacy paradox that postulates that the levels of privacy

concerns are not correlated to intended or actual privacy related behavior. Hence, the second main finding of the research negates the privacy paradox and postulates that the reported privacy concerns of consumers modify intended privacy related behavior.

Furthermore, it should be accentuated that the two main findings of this research are related. The enfeeblement of the privacy paradox stresses that the privacy related behavior of consumers is not as inconsistent as often is assumed. Hence, the lack of impact of the framing effects on a consistent decision is not remarkable.

In sum, the main finding of this research postulates that the privacy related behavior could be explained by the reported privacy concerns of consumers. This finding falsifies the privacy paradox, and hence refutes the anomaly between privacy attitude and privacy intended behavior. As a consequence, privacy related decision-making is compatible and therefore hard to influence by non-normative factors such as framing effects. These conclusions contribute to the existing literature as the findings are progressive and beg for reassessment of the fundamental principle in the research on information privacy: the privacy paradox.

5.2 Discussion of general conclusion

The central conclusion of this thesis thus postulates a correlation between privacy concerns and intended privacy related behavior. Subsequently, this study directly negates the main premise of the privacy paradox. This thesis is (to my best knowledge) the first study that shows direct evidence opposite to the privacy paradox and is therefore both noteworthy and progressive. Due to this remarkable conclusion, it is important to examine the difference between the utilized methods of inquiry of this study and other contemporary studies that endorse the privacy paradox.

Similar to contemporary studies that support the privacy ambiguity, this study adopted an online questionnaire to examine both the levels of privacy concerns of the respondents and the intended privacy related behavior. However, the utilized constructs to measure theses variables vary remarkably. A strong feature of this study is that it measures the variables in a more refined matter compared to other studies. For instance, the privacy concern variable is conducted by computing the average of the 7-point Likert-scale answer to four privacy concern related questions. Hence, lower privacy scores indicated more care for privacy and the difference in scores indicated different degrees in privacy concern. Contrary, earlier studies that also utilized the privacy concern measurement segmented their respondents into three categories. The privacy concern measurement was thus reduced to a categorical variable. Hence, the measurement became less punctual and the explanatory power of the variable is strongly reduced.

In addition, this study measured the intended behavior of the respondent in an extensive manner. First of all, not only the willingness to accept, a variable that measures the willingness of disclosing personal information, is questioned but also the willingness to pay. This two-jointed approach is unique in the realm of information privacy as earlier studies only examine a single dependent variable. For instance, Carrascal et al. (2013) stressed that individuals are only willing to pay a few Euro's to protect their private data. They concluded that this low valuation is in contrast with the general high levels of privacy concerns and the authors endorse the privacy paradox in their conclusion. Nevertheless, it has been theorized that the willingness to accept and willingness to pay are not identical and people tend to value their willingness to accept higher compared to their

willingness to pay. Hence, by focusing only on the willingness to pay the formulated conclusion might be questionable as the lack of correlation might be caused by the difference in willingness to pay and willingness to accept. The high levels of privacy concerns could be correlated with the (higher) general willingness to accept and therefore the study might draw their conclusions in an ill-considered manner.

Furthermore, contrary to other studies are the willingness to pay and the willingness to accept examined by a refined measurement. Both variables are measured by a close-ended question and the respondent could choose between 6 different answers ranging from not willing to accept/pay to willing to accept/pay more than €10. In addition, the answers between these extremes vary with €2.50. A consequence of this refined scale is that it provides detailed insights in the behavior of consumers. Earlier studies often measured the behavior of their consumers on a two-fold scale. The behavior could either confirm or negates the hypothesis did not account for different levels in these two types of behavior. For instance, (Beresford et al. 2002) categorized the behavior of their respondents as confirming or negating of the privacy paradox. Either the respondent could choose to buy a DVD for the discounted price and consequently forced to reveal the private data, or the respondent chooses to buy the DVD for the full price and protect the private data. The study does not allow for any levels of deviations and is therefore less precise compared to the current study.

All considered, it could be concluded that this study found a (positive) correlation between levels of privacy concerns and intended privacy related behavior. Other studies failed to reveal such a correlation and this discrepancy could be caused by the different measurement methods that are utilized. The present study not only examined both the willingness to accept and the willingness to pay, but in addition also used a more refined measurement.

5.3 Limitations of the research

Nevertheless, in spite of these refined measurements that are utilized by this study, there are several limitations and shortcomings of the research. These limitations are mostly caused by time and budget constraints but will nonetheless be discussed.

First of all, the sample of respondents is not representative for the actual population. As elaborated, the respondents are highly educated adolescents that are familiar with e-commerce. Due to the homogeneity of the sample, the outcomes could be distorted. For instance, the level of privacy concern of the actual population could be much higher and as a consequence the correlation can disappear. This concern is consistent with findings of earlier studies that postulated that highly educated people exhibit lower levels of privacy concerns (Youn and Hall, 2008). A first limitation of the research is therefore the homogeneity of the sample.

Contiguously, another limitation of the research is the fact that the online questionnaire examines the intended behavior of online consumers instead of the actual behavior. It could be possible that the intended behavior of consumers is inconsistent with their actual behavior. Staddon et al., (2013) emphasized on this disagreement en in their study they analyzed the difference between self-reported behavior and the actual behavior of Google+ users. The results accentuated that the self-reported behavior was more conservative than the actual behavior of the Google+ users. Hence, the result of this study could diminish when the actual behavior is measured instead of the intended behavior that is currently examined. Therefore, a second limitation of this research is fact that it analyzed the intended behavior.

Furthermore, the lack of impact of the framing effects could be caused by the design of the framing effects. By accentuating the positive and negative consequences of revealing personal information to a greater extent, the willingness to disclose personal information might be influenced. For instance, earlier studies have emphasized on the persuasive effect of pictures and reviews of others users (Duan, Gu and Whinston, 2008). Hence, it could be possible that the conducted framing effects are not persuasive enough and that a more extreme way of emphasizing benefits and costs influence the willingness to disclose the personal information. Consequently, a third limitation of the research is that the study only used three different framing effects, i.e. a positive, negative and neutral priming, and therefore not account for the strength of the primings.

5.4 Recommendations for future research

First of all, it is of major importance that future research continuous examining the validity of the privacy paradox. Current research on information privacy mostly assumes this validity and focuses on the different causes of the inconsistency. Nevertheless, as this research accentuates, the correctness of the privacy paradox is not as self-evident as often is assumed. Hence, future research should emphasize on analyzing the (lack of) correlation between privacy concern and actual behavior.

In addition, several recommendations are formulated inspired by the shortcomings of the present study. The main drawback of the research is the measurement intended behavior instead of the actual behavior of consumers. As elaborated, it could be possible that the actual behavior deviates from the intended behavior. If the actual behavior then fails to correlate to the privacy concerns of consumers, the privacy paradox is nonetheless correct. Therefore, future research is recommended to examine the relationship between privacy concerns and actual privacy related behavior.

A possible method that could be utilized to measure this actual behavior is the Becker-deGroot-Marschak mechanism. As emphasized, this is an incentive compatible open-ended question and due to budget constraints not utilized in the present study. The actual behavior of the respondent can then be measured and compared to the intended behavior as follow: First, the respondent completes a questionnaire similar to the survey utilized in this study. However, at the end of the questionnaire, the respondent is rewarded with a $5 gift card from Amazon.com. To receive the gift card, the participant is asked to fill in some personal information. The answer sheet contains several boxes and the respondent is able to fill in information ranching from gender to income. However, the respondent is not obliged to answer all the questions. Hence, the actual disclosure of personal information in exchange for 5 dollar can be compared to the reported willingness to accept and the willingness to pay. For instance, if the respondent answered in the previous section that his WTA for disclosing age, name and gender was 10 dollar and now disclose this type of personal information in exchange for 5 dollar, the respondent exhibit inconsistent behavior. In addition, another method to measure the actual privacy related behavior of individuals is to install special software on participants' computers that tracks behavior.

Furthermore, a prominent theory in behavioral economics is hedonic framing a concept coined by Richard Thaler (1985). Thaler accentuated in his article on a clarifying experiment named the "jacket-calculator saving" (Tversky & Kahneman 1985). The experiment learned that people are prepared to drive an extra 20 minutes to save $5 on a calculator that normally costs $15 but not for the jacket that costs $125. This conclusion emphasized an anomaly in standard economic theory as according to this reasoning the costs of the reduced item is alleged to be irrelevant. Hence, the disparity implied that "the utility of the saving must be associated with the

differences in values rather than the value of the difference" (Thaler, 1985 p. 186). Inspired by this conclusion, Thaler (1985) introduced the concept of hedonic framing, i.e. the way that individuals evaluate joint outcomes to maximize utility.

The importance of the principles of hedonic framing should not be underestimated. In the current study, respondents are shopping for a new set of headphone and the price for these headphones are around $30. Is the respondent still willing to reveal his personal information in exchange for a discount of $5 dollar when shopping for a new TV-set that costs around $1000? Future research should examine this inquiry by developing a questionnaire with different products.

As a final recommendation, upcoming research should examine if the privacy paradox is still renounced when a sample that is more representative for the population is utilized. As emphasized in the previous sections of this thesis, demographics influence the privacy concerns and the privacy related behavior of consumers. Hence, a more representative sample can control for these influences.

6 References

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce* (pp. 21-29). ACM.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, *2*(2005), 24-30.

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth?. *The Journal of Legal Studies*, *42*(2), 249-274.

Alatalo, T., & Siponen, M. T. (2001). Addressing the personalization paradox in the development of electronic commerce systems. In *Post-proceedings of the EBusiness. Research Forum (eBRF), Tampere, Finland*.

Allen, I. E., & Seaman, C. A. (2007). Likert scales and data analyses. *Quality progress*, *40*(7), 64.

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

Baek, Y. M. (2014). Solving the privacy paradox: A counter-argument experimental approach. *Computers in Human Behavior*, *38*, 33-42.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9).

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.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly*, *35*(4), 1017-1042.

Beldad, A. D., De Jong, M., & Steehouder, M. F. (2009). When the bureaucrat promises to safeguard your online privacy: Dissecting the contents of privacy statements on Dutch municipal websites. *Government Information Quarterly*,*26*(4), 559-566.

Beresford, A. R., Kübler, D., & Preibusch, S. (2012). Unwillingness to pay for privacy: A field experiment. *Economics Letters*, *117*(1), 25-27.

Berger, D. D. (2011). Balancing consumer privacy with behavioral targeting. *Santa Clara Computer and High Technology Law Journal*, *27*, 3.

Bleier, A., & Eisenbeiss, M. (2015). The importance of trust for personalized online advertising. *Journal of Retailing*, *91*(3), 390-409.

Boone, H. N., & Boone, D. A. (2012). Analyzing likert data. *Journal of extension*,*50*(2), 1-5.

Brown, B. (2001). Studying the internet experience. *HP LABORATORIES TECHNICAL REPORT HPL*, (49).

Carrascal, J. P., Riederer, C., Erramilli, V., Cherubini, M., & de Oliveira, R. (2013). Your browsing behavior for a big mac: Economics of personal information online. In *Proceedings of the 22nd international conference on World Wide Web* (pp. 189-200). ACM.

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

Cho, H., Lee, J. S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, *26*(5), 987-995.

Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). A multinational study on online privacy: global concerns and local responses. *New media & society*, *11*(3), 395-416.

Consumers-Union, . (2008). Consumer reports poll: Americans extremely concerned about Internet privacy.

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

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of social issues*, *59*(2), 323-342.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83-108.

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

Egelman, S., Felt, A. P., & Wagner, D. (2013). Choice architecture and smartphone privacy: There'sa price for that. In *The economics of information security and privacy* (pp. 211-236). Springer Berlin Heidelberg.

Forbes (2016): http://www.forbes.com/forbes/welcome/?toURL=http://www.forbes.com/companies/google/&refURL=https://www.google.nl/&referrer=https://www.google.nl/

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

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

Hann, I. H., Hui, K. L., Lee, S. Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach.*Journal of Management Information Systems*, *24*(2), 13-42.

Hansell, S. (2008a). Google fights for the right to hide its privacy policy. *The New York Times*.

Hansell, S. (2008b). Is Google violating a California privacy law. *The New York Times*.

Hinz, O., Hann, I. H., & Spann, M. (2011). Price discrimination in e-commerce? An examination of dynamic pricing in name-your-own price markets. *Mis quarterly*, *35*(1), 81-98.

Horowitz, J. K., & McConnell, K. E. (2002). A review of WTA/WTP studies.*Journal of environmental economics and Management*, *44*(3), 426-447.

Huberman, B. A., Adar, E., & Fine, L. R. (2005). Valuating privacy. *IEEE Security & Privacy*, *3*(5), 22-25.

Hughes-Roberts, T. (2013). Privacy and Social Networks: Is Concern a Valid Indicator of Intention and Behaviour?. In *Social Computing (SocialCom), 2013 International Conference on* (pp. 909-912). IEEE.

Hui, K. L., Tan, B. C., & Goh, C. Y. (2006). Online information disclosure: Motivators and measurements. *ACM Transactions on Internet Technology (TOIT)*, *6*(4), 415-441.
Janssens, W., De Pelsmacker, P., & Van Kenhove, P. (2008). *Marketing research with SPSS*. Pearson Education.

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: self-reports versus observed behavior. *International Journal of Human-Computer Studies*, *63*(1), 203-227.

Johnson, E. J., Bellman, S., & Lohse, G. L. (2002). Defaults, framing and privacy: Why opting in-opting out1. *Marketing Letters*, *13*(1), 5-15.

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

Kahneman, D., & Tversky, A. (1984). Choices, values, and frames. *American psychologist*, *39*(4), 341.

Kahneman, D., Knetsch, J. L., & Thaler, R. H. (1991). Anomalies: The endowment effect, loss aversion, and status quo bias. *The journal of economic perspectives*, *5*(1), 193-206.

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

Knetsch, J. L., & Sinden, J. A. (1984). Willingness to pay and compensation demanded: Experimental evidence of an unexpected disparity in measures of value. *The Quarterly Journal of Economics*, 507-521.

Knijnenburg, B. P., & Kobsa, A. (2013). Making decisions about privacy: information disclosure in context-aware recommender systems. *ACM Transactions on Interactive Intelligent Systems (TiiS)*, *3*(3), 20.

Kokolakis, S. (2015). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*.

Lee, C. H., & Cranage, D. A. (2011). Personalisation–privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel Web sites. *Tourism Management*, *32*(5), 987-994.

Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk.*International Journal of Human-Computer Studies*, *71*(9), 862-877.

Levin, I. P., & Gaeth, G. J. (1988). How consumers are affected by the framing of attribute information before and after consuming the product. *Journal of consumer research*, *15*(3), 374-378

Levin, I. P., Schneider, S. L., & Gaeth, G. J. (1998). All frames are not created equal: A typology and critical analysis of framing effects. *Organizational behavior and human decision processes*, *76*(2), 149-188.

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*,*51*(1), 62-71.

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

Likert, R. (1932). A technique for the measurement of attitudes. *Archives of psychology*.

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.

Maxwell, S. E., & Delaney, H. D. (2004). *Designing experiments and analyzing data: A model comparison perspective* (Vol. 1). Psychology Press.

McCrum-Gardner, E. (2008). Which is the correct statistical test to use?. *British Journal of Oral and Maxill*

McGuire, T., Manyika, J., & Chui, M. (2012). Why big data is the new competitive advantage. *Ivey Business Journal*, *76*(4), 1-4.

Meinert, D. B., Peterson, D. K., Criswell, J. R., & Crossland, M. D. (2006). Would regulation of web site privacy policy statements increase consumer trust?. *Informing Science*, *9*, 123.

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization science*, *11*(1), 35-57.

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.

Orenga-Roglá, S., & Chalmeta, R. (2016). Social customer relationship management: taking advantage of Web 2.0 and Big Data technologies.*SpringerPlus*, *5*(1), 1462.

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

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

Sheehan, K. B. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing*, *13*(4), 24-38.

Simon, H. A. (1982). *Models of bounded rationality: Empirically grounded economic reason* (Vol. 3). MIT press.

Simon, R. (2008). Relentless: How Barack Obama Outsmarted Hillary Clinton. *Politico. com. Washington, DC August*, *25*.

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2004). Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk analysis*, *24*(2), 311-322.

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

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

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM conference on Electronic Commerce* (pp. 38-47). ACM.

Staddon, J., Acquisti, A., & LeFevre, K. (2013, September). Self-reported social network behavior: Accuracy predictors and implications for the privacy paradox. In *Social Computing (SocialCom), 2013 International Conference on* (pp. 295-302). IEEE.

Statistia (2016): https://www.statista.com/markets/413/e-commerce/

Stone, B., & Stelter, B. (2009). Facebook backtracks on use terms. *The New York Times B*, *1*, B6.

Sundar, S. S., & Marathe, S. S. (2010). Personalization versus customization: The importance of agency, privacy, and power usage. *Human Communication Research*, *36*(3), 298-322.

Sundar, S. S., Kang, H., Wu, M., Go, E., & Zhang, B. (2013). Unlocking the privacy paradox: do cognitive heuristics hold the key?. In *CHI'13 Extended Abstracts on Human Factors in Computing Systems* (pp. 811-816). ACM.

Syre, S., & Stein, C., (2001, June 21).You should know who's selling your information. *Boston Globe*, p. C1.

Tam, K. Y., & Ho, S. Y. (2005). Web personalization as a persuasion strategy: An elaboration likelihood model perspective. *Information Systems Research*,*16*(3), 271-291.

Thaler, R. (1980). Toward a positive theory of consumer choice. *Journal of Economic Behavior & Organization*, *1*(1), 39-60.

Thaler, R. (1985). Mental accounting and consumer choice. *Marketing science*, *4*(3), 199-214.

Thaler, R., & Sunstein, C. (2008). Nudge: The gentle power of choice architecture. *New Haven, Conn.: Yale*.

Thaler, R. H., Sunstein, C. R., & Balz, J. P. (2014). Choice architecture. *The behavioral foundations of public policy*.

Tversky, A., & Kahneman, D. (1975). Judgment under uncertainty: Heuristics and biases. In *Utility, probability, and human decision making* (pp. 141-162). Springer Netherlands.

Tversky, A., & Kahneman, D. (1985). The framing of decisions and the psychology of choice. In *Environmental Impact Assessment, Technology Assessment, and Risk Analysis* (pp. 107-129). Springer Berlin Heidelberg.

Tversky, A., & Thaler, R. H. (1990). Anomalies: preference reversals. *The Journal of Economic Perspectives*, *4*(2), 201-211.

Vail, M. W., Earp, J. B., & Antón, A. I. (2008). An empirical study of consumer perceptions and comprehension of web site privacy policies. *IEEE Transactions on Engineering Management*, *55*(3), 442-454.

Westin, A (1991). Harris-Equifax consumer privacy survey 1991. *Atlanta, GA: Equifax Inc*.

Westin, A. (2001). Opinion surveys: What consumers have to say about information privacy. *Prepared Witness Testimony, The House Committee on Energy and Commerce*.

Wilkinson, N., & Klaes, M. (2012). *An introduction to behavioral economics*. Palgrave Macmillan.

Xie, E., Teo, H. H., & Wan, W. (2006). Volunteering personal information on the internet: Effects of reputation, privacy notices, and rewards on online consumer behavior. *Marketing letters*, *17*(1), 61-74.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *ICIS 2008 proceedings*, 6.

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

Youn, S., & Hall, K. (2008). Gender and online privacy among teens: Risk perception, privacy concerns, and protection behaviors. *Cyberpsychology & behavior*, *11*(6), 763-765.

Zafeiropoulou, A. M., Millard, D. E., Webber, C., & O'Hara, K. (2013, May). Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions?. In *Proceedings of the 5th Annual ACM Web Science Conference* (pp. 463-472). ACM.

7 Appendix

1. Overview of main and sub-hypotheses and results

Overview hypotheses and results

H1		Highlighting the advantages of revealing personal information in an online environment enhances the willingness to accept of consumers.	No
	H1a	Highlighting the advantages of revealing the personal information in an online environment enhances the difference between the general willingness to accept and the post priming willingness to accept of consumers.	No
	H1b	Highlighting the advantages of revealing the personal information in an online environment enhances the willingness to accept of consumers controlling for their general willingness to accept.	No
	H1c	Highlighting the advantages of revealing the personal information in an online environment enhances the difference between the general willingness to accept and the post priming willingness to accept, controlling for the general willingness to accept.	No
	H1d	Highlighting the advantages of revealing the personal information in an online environment enhances the willingness to accept, controlling for their privacy concerns.	No
	H1e	Highlighting the advantages of revealing the personal information in an online environment enhances the difference between the general willingness to accept and their post priming willingness to accept, controlling for their privacy concerns	No
H2		Highlighting the disadvantages of revealing personal information in an online environment enhances the willingness to accept of consumers.	No
	H2a	Highlighting the disadvantages of revealing the personal information in an online environment enhances the difference between the general willingness to accept and the post priming willingness to accept of consumers.	No
	H2b	Highlighting the disadvantages of revealing the personal information in an online environment enhances the willingness to accept of consumers controlling for their general willingness to accept.	No
	H2c	Highlighting the disadvantages of revealing the personal information in an online environment enhances the difference between the general willingness to accept and the post priming willingness to accept, controlling for the general willingness to accept.	No
	H2d	Highlighting the disadvantages of revealing the personal information in an online environment enhances the willingness to accept, controlling for their privacy concerns.	No
	H2e	Highlighting the disadvantages of revealing the personal information in an online environment enhances the difference between the general willingness to accept and their post priming willingness to accept, controlling for their privacy concerns	No
H3		The willingness to accept is higher for the consumers that are either positively of	No

negatively primed compared to the willingness to accept of consumers that are not primed.

H4	The general willingness to accept of the respondents is higher compared to their general willingness to pay	Accepted
H5	The privacy concern of consumers is not explanatory for the general willingness to accept of consumers.	No

By conducting an ANCOVA analysis, the differences between the post-priming willingness to accept could be measured controlling for either privacy concerns or general willingness to accept. Again, no significant differences were reported. The statistical output of one of these analyses is given below.

Univariate analysis of Variance – Test of between subject effects

Dependent Variable: Willingness To Accept

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	49.986a	4	12.496	3.292	.014	.104
Intercept	46.515	1	46.515	12.253	.001	.098
GWTA	41.183	1	41.183	10.849	.001	.088
Privacy_Concerns	.072	1	.072	.019	.891	.000
Condition	.599	2	.300	.079	.924	.001
Error	428.972	113	3.796			
Total	2797.000	118				
Corrected Total	478.958	117				

a. R Squared = .104 (Adjusted R Squared = .073)

2. Overview of online questionnaire

Intro Dear respondent,

First of all, thank you for participating! This study is part of my Master Thesis written at the Erasmus University Rotterdam and takes approximately 3 minutes to complete. Please keep in mind that there are no right or wrong answers and that your responses are allowed to deviate during the survey.
If you have any questions, please feel free to contact me at 433011vk@student.eur.nl.

Once again, thank you for your contribution to my thesis.

Best, Vita van der Kraaij

Click the next button to get started!

Q1 I am concerned about my privacy in everyday life.

- ❍ Strongly agree (1)
- ❍ Agree (2)
- ❍ Somewhat agree (3)
- ❍ Neither agree nor disagree (4)
- ❍ Somewhat disagree (5)
- ❍ Disagree (6)
- ❍ Strongly disagree (7)

Q2 I am concerned about privacy theft.

- ❍ Strongly agree (1)
- ❍ Agree (2)
- ❍ Somewhat agree (3)
- ❍ Neither agree nor disagree (4)
- ❍ Somewhat disagree (5)
- ❍ Disagree (6)
- ❍ Strongly disagree (7)

Q3 I am concerned about my privacy online.

- ❍ Strongly agree (1)
- ❍ Agree (2)
- ❍ Somewhat agree (3)
- ❍ Neither agree nor disagree (4)
- ❍ Somewhat disagree (5)
- ❍ Disagree (6)
- ❍ Strongly disagree (7)

Q4 I am likely to read the privacy policy of an e-commerce website before buying anything.

- Strongly agree (1)
- Agree (2)
- Somewhat agree (3)
- Neither agree nor disagree (4)
- Somewhat disagree (5)
- Disagree (6)
- Strongly disagree (7)

Q5 Privacy policies accurately reflect what companies do.

- Strongly agree (1)
- Agree (2)
- Somewhat agree (3)
- Neither agree nor disagree (4)
- Somewhat disagree (5)
- Disagree (6)
- Strongly disagree (7)

Q4 These days, some online retailers are offering their (potential) customers a small discount in exchange for disclosing personal information. How much discount should an online-retailer offer you to reveal your:full-name, e-mail address, age and gender?

- I do not require a compensation to reveal my personal information. (1)
- 0 - € 2.50 (2)
- € 2.50 - € 5 (3)
- € 5 - € 7.50 (4)
- € 7.50 - € 10 (5)
- more than € 10 (6)
- I am not willing to reveal my personal information for any given discount. (7)

Q5 How often do you make online purchases?

- More than 3 times a month (1)
- 2-3 times a month (2)
- Once a month (3)
- Less than once a month (4)
- Never (5)

Q6 What is your gender?

- Male (1)
- Female (2)

Q7 What is your age?

- Under 18 (1)
- 18 - 24 (2)
- 25 - 34 (3)
- 35 - 44 (4)
- 45 - 54 (5)
- 55 - 64 (6)
- Older than 65 (7)

Q8 What is the highest level of education you have completed?

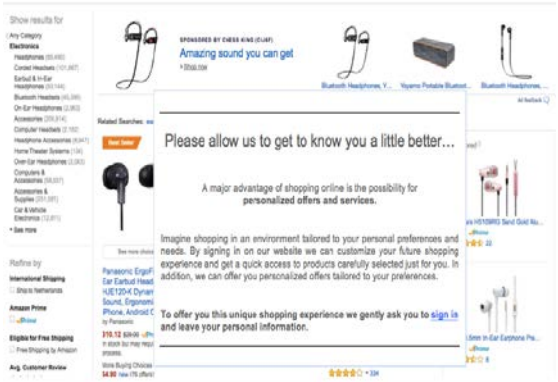
- High school (1)
- Bachelor degree University of Applied Science (2)
- Bachelor degree Research University (3)
- Master degree Research Univerisity (4)
- PhD (5)

Q9 **Many online retailers use your personal information for divergent purposes, e.g. price discrimination, marketing purposes or sell your data to third parties. Suppose you are given the opportunity to ensure an anonymous shopping experience by utilising a pseudonym in the form of a number. Hence, you are not obliged to reveal any personal information such as full-name, e-mail address, age nor gender to the online-retailer. How much are you willing to pay for this one time service?**

- I am not willing to pay any commission for this type of service. (1)
- 0 - € 2.50 (2)
- € 2.50 - € 5 (3)
- € 5 - € 7.50 (4)
- € 7.50 - €10 (5)
- More than € 10 (6)

Q10 **Imagine you are shopping online for a new set of headphones.While screening the assortment of an online-retailer the following pop-up appears in your screen.Please read the pop-up carefully before answering the next question.**

Q11

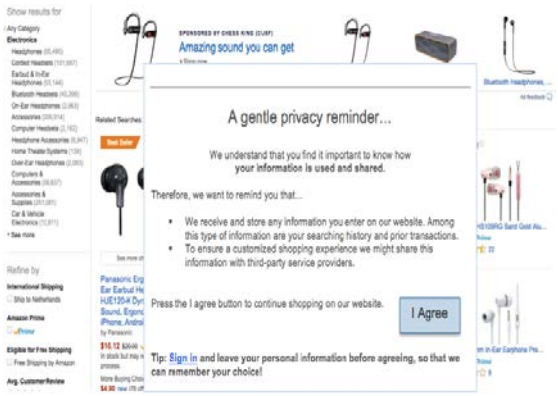


Q12 **Some retailers are offering a small discount in exchange for revealing some personal information. For instance, consider the discount coupons that some retailers reward you with after subscribing to the newsletter. How much discount should this particular retailer offer you to sign in and reveal your:full-name, e-mail address, age and gender?** I do not require a compensation to reveal my personal information. (1)

- 0 - € 2.50 (2)
- € 2.50 - € 5 (3)
- € 5 - € 7.50 (4)
- € 7.50 - € 10 (5)
- More than € 10 (6)
- I am not willing to reveal my personal information for any given discount. (7)

Q13 **Imagine you are shopping online for a new set of headphones. While screening the assortment of an online-retailer a pop-up appears in your screen.Please read the pop-up carefully before answering the next question**.

Q14

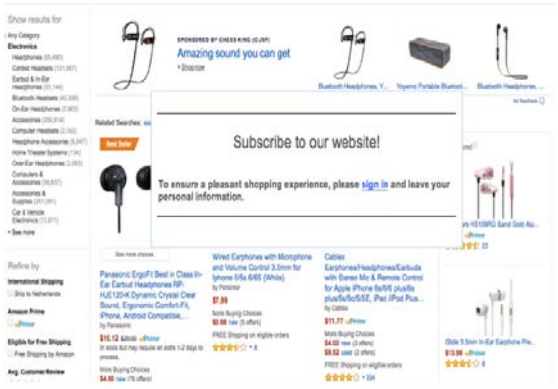


Q15 **Some retailers are offering a small discount in exchange for revealing some personal information. For instance, consider the discount coupons that some retailers reward you with after subscribing to the newsletter. How much discount should this particular retailer offer you to sign in and reveal your:full-name, e-mail address, age and gender?**

- I do not require a compensation to reveal my personal information. (1)
- 0 - € 2.50 (2)
- € 2.50 - € 5 (3)
- € 5 - € 7.5 (4)
- € 7.5 - € 10 (5)
- More than € 10 (6)
- I am not willing to reveal my personal information for any given discount. (7)

Q16 **Imagine you are shopping online for a new set of headphones. While screening the assortment of an online-retailer a pop-up appears in your screen. Please read the pop-up carefully before answering the next question.**

Q17

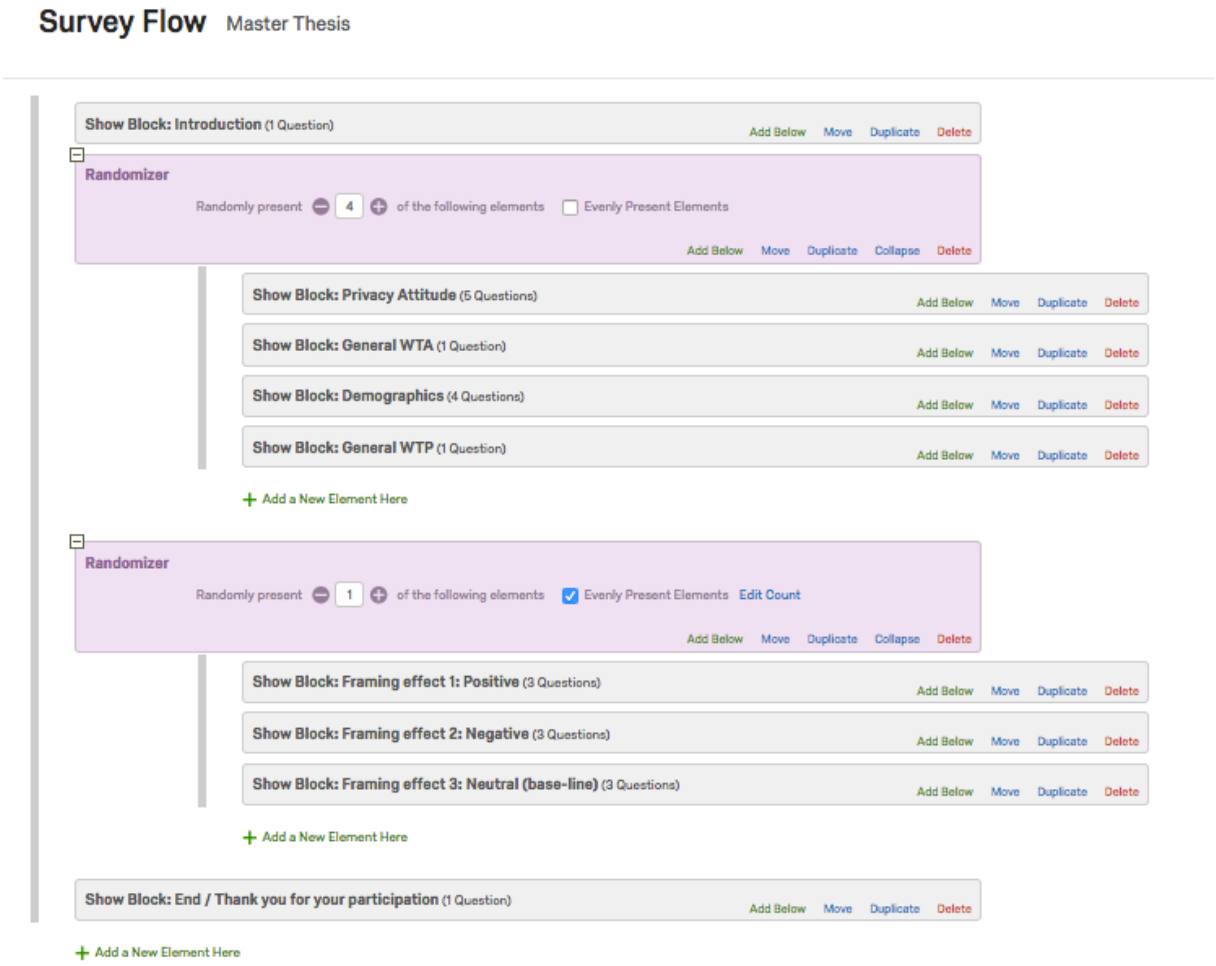


Q18 **Some retailers are offering a small discount in exchange for revealing some personal information. For instance, consider the discount coupons that some retailers reward you with after subscribing to the newsletter. How much discount should this particular retailer offer you to sign in and reveal your:full-name, e-mail address, age and gender?**

- I do not require a compensation to reveal my personal information. (1)
- 0 - € 2.50 (2)
- € 2.50 - € 5 (3)
- € 5 - € 7.5 (4)
- € 7.5 - € 10 (5)
- More than € 10 (6)
- I am not willing to reveal my personal information for any given discount. (7)

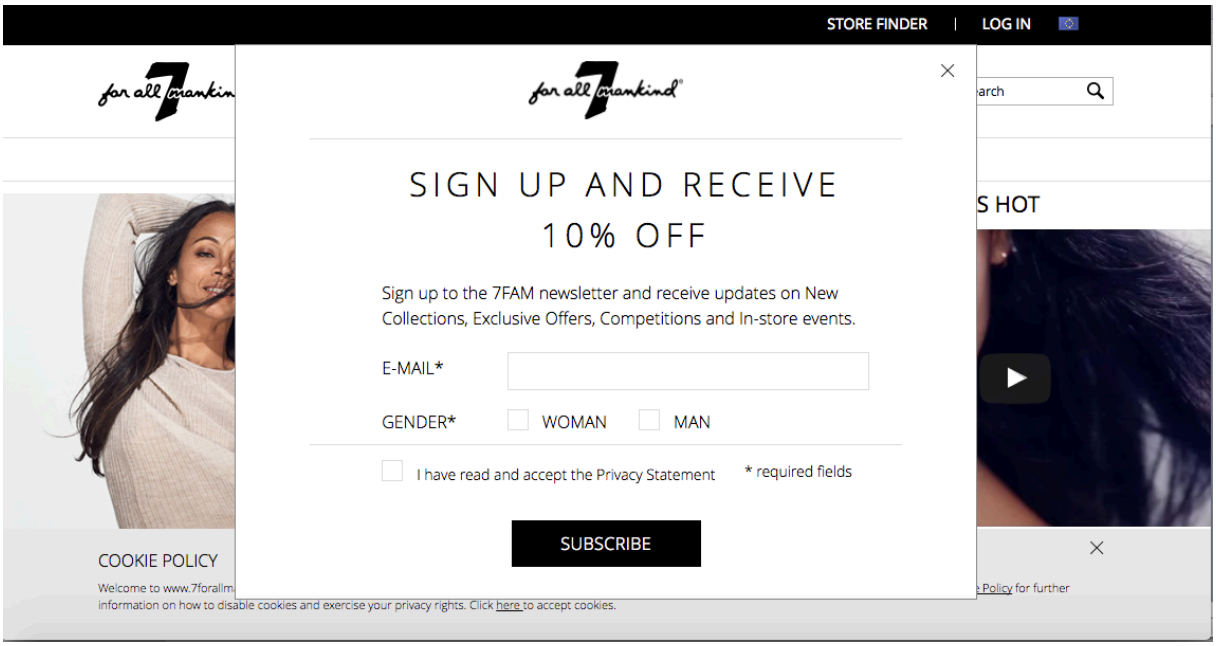
Q19 **This is the end of the questionnaire.Thank you for your participation!**

3. **<u>Survey flow of questionnaire that includes randomization</u>**

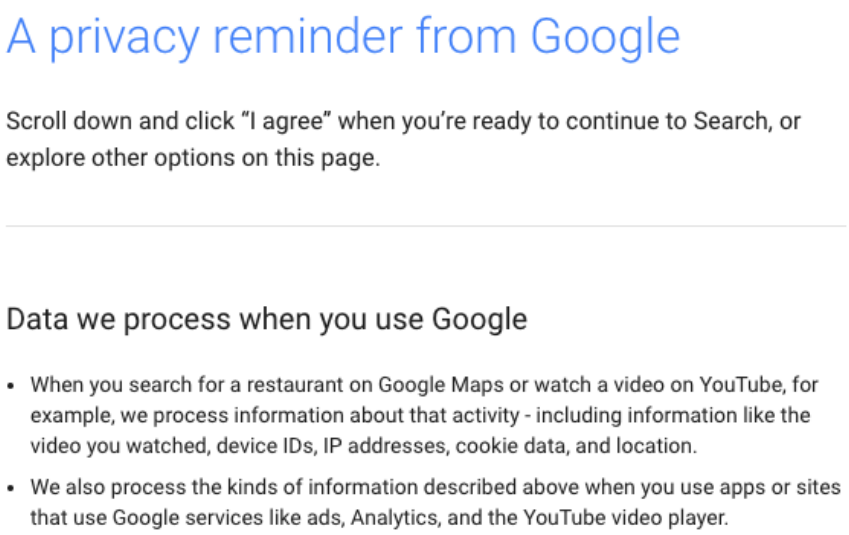


4. **<u>Inspiration for framing effects.</u>**

1. Real pop up utilized by jeans brand “Seven for all mankind”

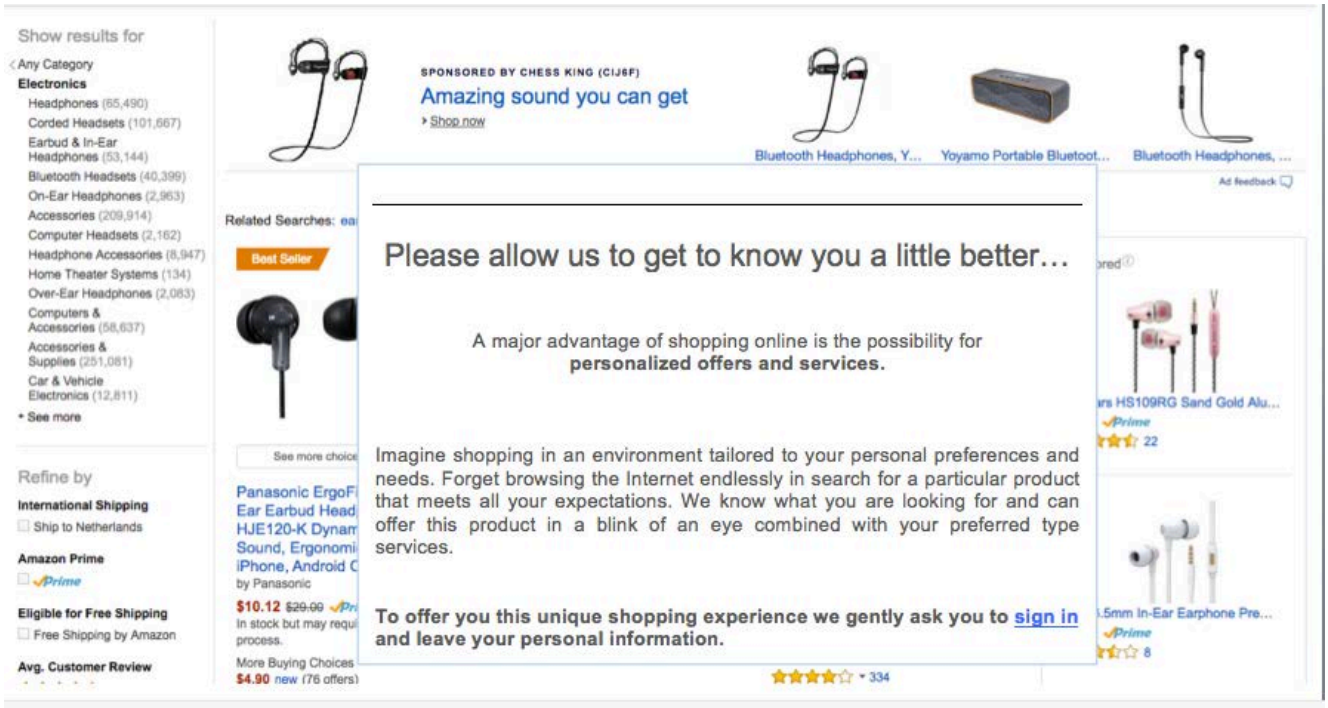


2. Content of privacy statement Google

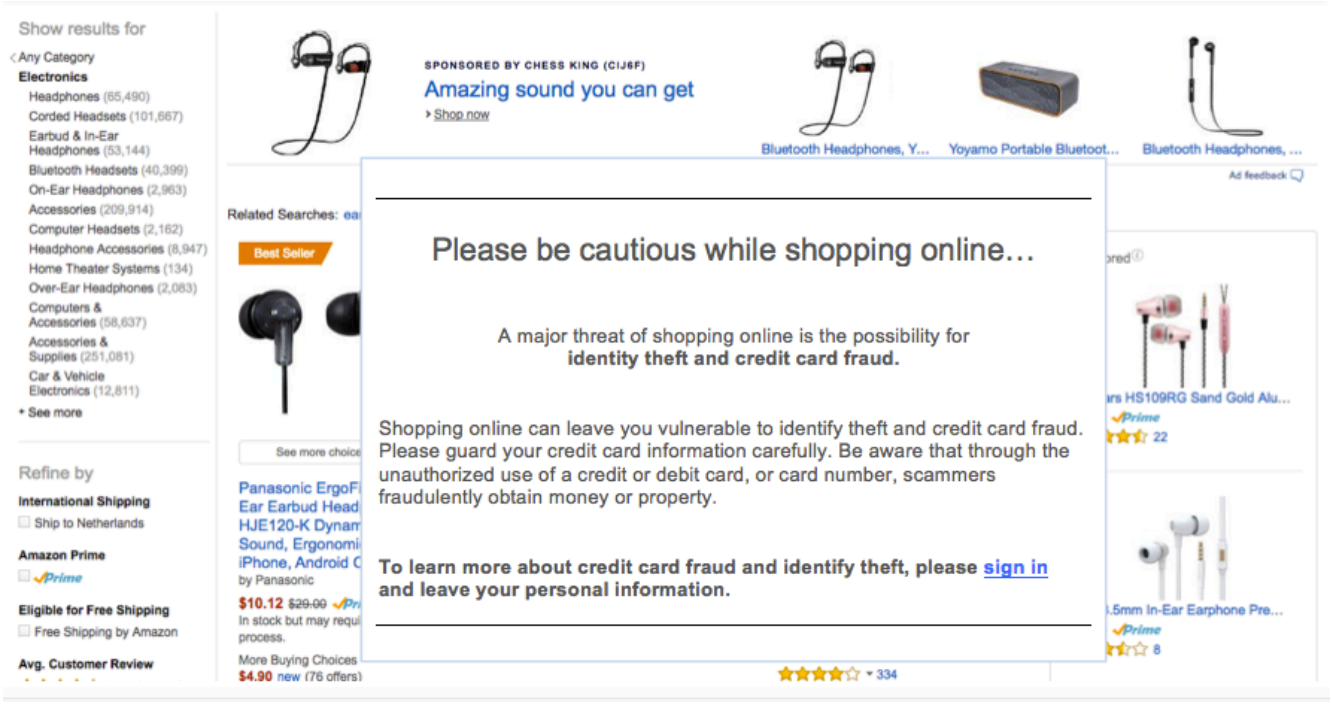


5. Outlook framing effects

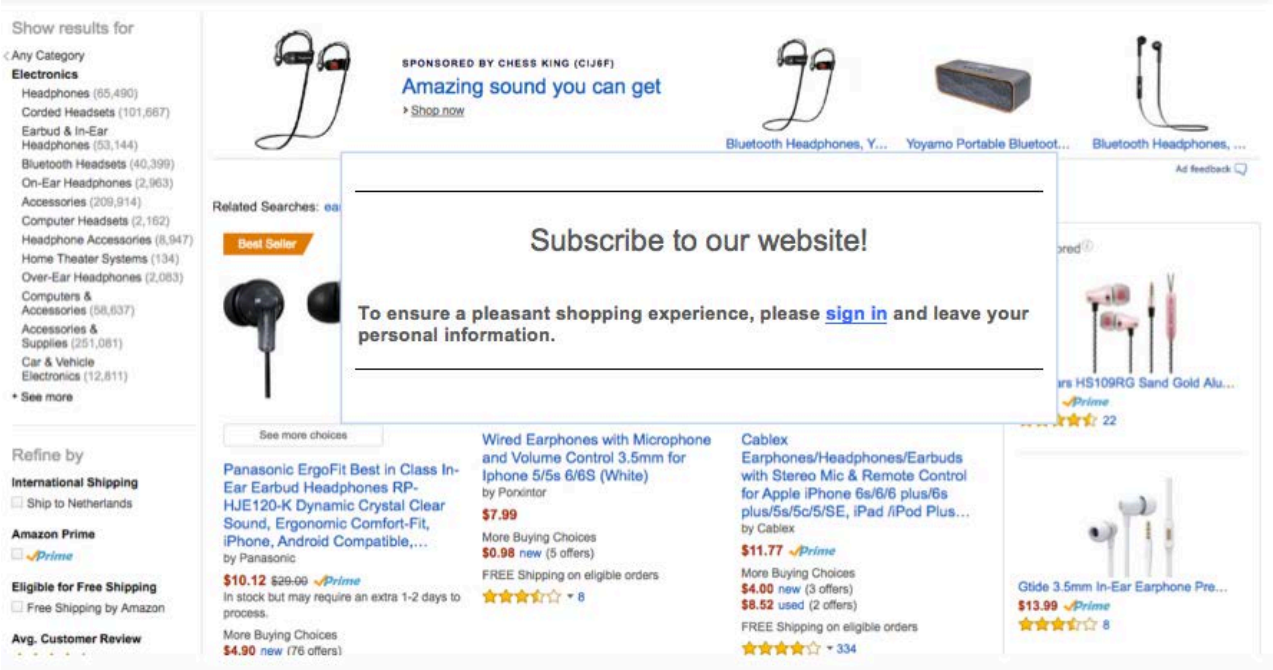
Framing 1 / Positive: Highlighting the advantages of sharing personal information online.



Framing 2 / Negative: Highlighting the risks (i.e. a disadvantages) of revealing personal information.



Framing 3 / Neutral: Highlighting no negative or positive aspects of revealing personal information online.



6. The privacy concern measurement

Inter Item - Correlation Matrix

	Q1	Q2	Q3	Q4	Q5
Q1	-	.545	.508	.256	-.005
Q2	.545	-	.552	.332	-.170
Q3	.508	.552	-	.282	-.282
Q4	.256	.332	.282	-	-.018
Q5	-.005	-.170	-.282	-.018	-

Q1 - I am concerned about my privacy in everyday life.

Q2 - I am concerned about privacy theft.

Q3 - I am concerned about my privacy online.

Q4 - I am likely to read the privacy policy of an e-commerce website before buying anything.

Q5 - Privacy policies accurately reflect what companies do.

Reliability statistics (N = 5)

Cronbach's Alpha	Cronbach's Alpha (Stand. Items)	N of Items
.567	.556	5

Reliability statistics (N = 4)

Cronbach's Alpha	Cronbach's Alpha (Stand. Items)	N of Items
.738	.737	4

→ By excluding question 5 the Cronbach's Alpha increases to a significant level (Cronbach's $\alpha \geq .7$)

Furthermore, the privacy concern measurement is the average of the answer to the 4 different questions.

7. Control variable

Type of analysis: Descriptive Statistics, Frequencies.

Control Variable - Gender			Control Variable - Age		
	Frequency	*Percent*		*Frequency*	*Percent*
Female	74	62,7	18 – 24	36	30,5
Male	44	37,3	25 – 34	82	69,5
Total	118	100%	Total	118	100%

Control Variable - Education			Control Variable - Online purchase frequency		
	Frequency	*Percent*		*Frequency*	*Percent*
High school	25	*21,2*	More than 3 times a month	25	*21,2*
Bachelor degree HBO	40	*33,9*	2 – 3 times a month	40	*33,9*
Bachelor degree WO	21	17,8	Once a month	32	*27,1*
Master degree WO	54	45,8	Less than once a month	21	*17,8*
PhD	1	0,8			
Total	100	100	Total	118	*100*

8. Remaining Variables

Type of analysis: Descriptive Statistics

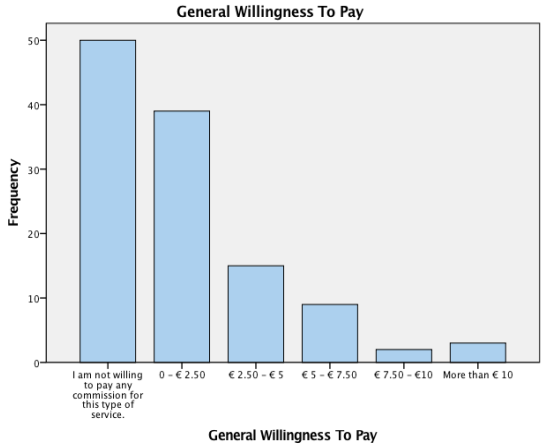
Descriptive Statistics - Variables

	N	Minimum	Maximum	Mean	Std. Deviation
Privacy Concern	118	1.50	6.50	3.8030	1.11509
General Willingness to accept	118	1	7	4.24	1.973
General Willingness to pay	118	1	6	2.01	1.195
Willingness to accept post priming	118	1	7	4.43	2.023

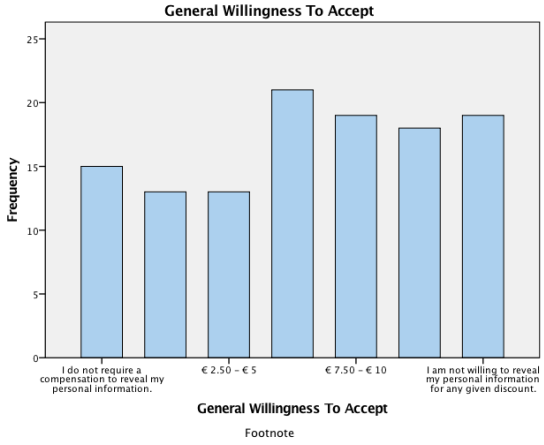
Descriptive Statistics – Willingness to accept post priming

	N	Minimum	Maximum	Mean	Std. Deviation
WTA 1 (Positive framing)	38	1	7	4.34	1.963
WTA 2 (Negative framing)	39	1	7	4.31	2.129
WTA 3 (Neutral framing)	41	1	7	4.63	2.009

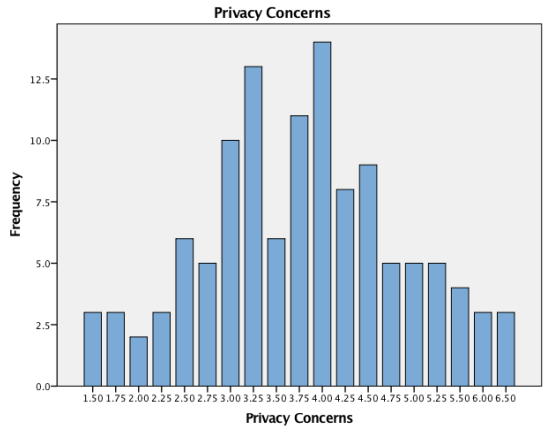
Bar Chart frequency Count – GTWP / GWTA / PC / WTA1 / WTA2 / WTA3



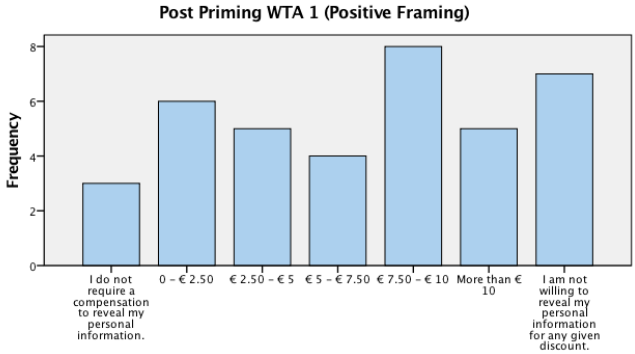
GWTP Median: 2.00



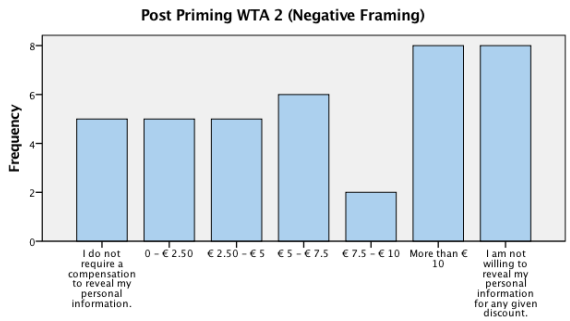
GWTA Median: 4.00



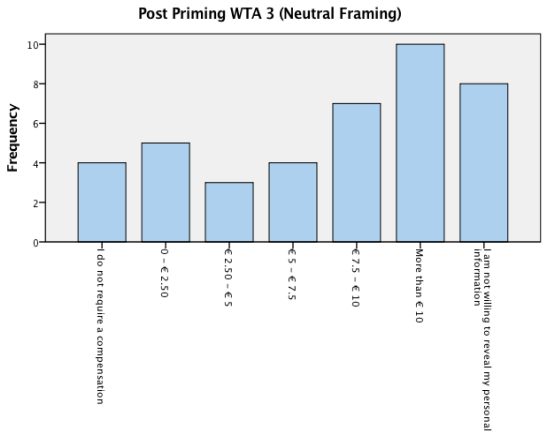
PC Mean 3.80 Std. Deviation: 1.973



WTA 1 Median: 5.00



WTA2 Median: 4.00



WTA3 Median: 5.00

9. <u>Randomization of the control variable</u>

Type of analysis: (Pearson) Chi-square analysis.

Count – Condition * Gender

		Female	Male	Total
Condition	Positive	22	16	38
	Negative	28	11	39
	Neutral	24	17	41
Total		74	44	118

Chi-Square Tests – Condition * Gender

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	2.059a	2	.357
Likelihood Ratio	2.106	2	.349
Linear-by-Linear Association	.001	1	.978
N of Valid Cases	118		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 14.17.

Count – Condition * Age

		18 - 24	25 - 34	Total
Condition	Positive	11	27	38
	Negative	14	25	39
	Neutral	11	30	41
Total		36	82	118

Chi-Square Tests – Condition * Age

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	.840a	2	.657
Likelihood Ratio	.831	2	.660
Linear-by-Linear Association	.050	1	.824
N of Valid Cases	118		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 11.59.

Count – Condition * Online purchase frequency

		More than 3 times a month	2-3 times a month	Once a month	Less than once a month	Total
Condition	Positive	7	12	10	9	38
	Negative	11	17	9	2	39
	Neutral	7	11	13	10	41
Total		25	40	32	21	118

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 6.76.

Chi-Square Tests – Condition * Online purchase frequency

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	8.938[a]	6	.177
Likelihood Ratio	10.048	6	.123
Linear-by-Linear Association	.173	1	.677
N of Valid Cases	118		

Chi-Square Tests – Condition * Education

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	2.838a	8	.944
Likelihood Ratio	3.006	8	.934
Linear-by-Linear Association	.094	1	.759
N of Valid Cases	118		

a. 6 cells (40.0%) have expected count less than 5. The minimum expected count is .32.

Count – Condition * Education

		High school	Bachelor degree University of Applied Science	Bachelor degree Research University	Master degree Research Univerisity	PhD	Total
Condition	Positive	5	8	6	18	1	38
	Negative	5	9	7	18	0	39
	Neutral	4	11	8	18	0	41
Total		14	28	21	54	1	118

10. <u>Statistical output Output of the One-way ANOVA analysis to test the three conditions on the post priming willingness to accept post priming (WTA)</u>

Descriptive Statistics – Willingness to accept post priming

	N	Mean	Std. Deviation	Std. Error	95% confidence interval for Mean		Min	Max
					Lower Bound	Upper Bound		
Positive framing	38	4.34	1.963	.318	3.70	4.99	1	7
Negative framing	39	4.31	2.129	.341	3.62	5.00	1	7
Neutral framing	41	4.63	2.009	.314	4.00	5.27	1	7
Total	118	4.43	2.023	.186	4.06	4.80	1	7

Test of Homogeneity of Variances

Willingness to accept post priming

Levene Statistic	df1	Df2	Sig.
.378	2	115	.686

ANOVA

Willingness to accept post priming

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	2.585	2	1.293	.312	.733
Within Groups	476.373	115	4.142		
Total	478.958	117			

Contrast Tests

Willingness to accept post priming	Contrast	Value of Contrast	Std. Error	t	df	Sig. (2-tailed)
Assume equal variances	1	-.29	.458	-.637	115	.525
	2	-.33	.455	-.717	115	.475
	3	-.62	.787	-.786	115	.434
Does not assume equal variances	1	-.29	.447	-.653	76.780	.516
	2	-.33	.463	-.704	77.093	.483
	3	-.62	.782	-.791	82.878	.431

11. One- Sample T-test to examine the significance of delta WTA.

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
Delta WTA	118	.1949	2.32878	.21438

One-Sample Statistics – Test Value = 0

					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
Delta WTA	.909	117	.365	.19492	-.2297	.6195

12. Output of the One-way ANOVA analysis to test the three conditions on the difference between GWTA and post WTA (Delta WTA).

Descriptive Statistics – delta WTA

					95% confidence interval for mean			
	N	Mean	Std. Deviation	Std. Error	Lower Bound	Upper Bound	Min	Max
Positive framing	38	.1053	2.46916	.40055	-.7063	.9169	-5.00	6.00
Negative framing	39	.4615	2.61419	.41861	-.3859	1.3090	-6.00	6.00
Neutral framing	41	.0244	1.90378	.29732	-.5765	.6253	-4.00	6.00
Total	118	.1949	2.32878	.21438	-.2297	.6195	-6.00	6.00

Test of Homogeneity of Variances

Delta WTA

Levene Statistic	df1	Df2	Sig.
1.715	2	115	.185

ANOVA

Delta WTA

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	4.270	2	2.135	.390	.678
Within Groups	630.247	115	5.480		
Total	634.517	117			

Contrast Tests

Willingness to accept post priming	Contrast	Value of Contrast	Std. Error	t	df	Sig. (2-tailed)
Assume equal variances	1	.0809	.52715	.153	115	.878
	2	.4371	.52363	.835	115	.406
	3	.5180	.90522	.572	115	.568
Does not assume equal variances	1	.0809	.49884	.162	69.491	.872
	2	.4371	.51345	.851	69.265	.397
	3	.5180	.83022	.624	102.622	.534

13. Out-put of the Non-parametric Kruskal Wallis test

Test Statistics – Kruskal Wallis

	Post_WTA
Chi-Square	.571
df	2
Asymp. Sig.	.752

a. Kruskal Wallis Test

b. Grouping Variable: Condition

Kruskal Wallis test - Ranks

	Condition	N	Mean Rank
Post_WTA	Positive	38	57.70
	Negative	39	57.87
	Neutral	41	62.72
	Total	118	

14. Out-put of Simple Linear regression

Model Summary Linear Regression – Privacy Concern * GWTA

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
	.293a	.086	.078	1.894

a. Predictors: (Constant), Privacy Concerns

ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	39.164	1	39.164	10.916	.001b
	Residual	416.192	116	3.588		
	Total	455.356	117			

a. Dependent Variable: General Willingness To Accept

b. Predictors: (Constant), Privacy Concerns

Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	6.210	.622		9.982	.000
	Privacy Concerns	-.519	.157	-.293	-3.304	.001

a. Dependent Variable: General Willingness To Accept