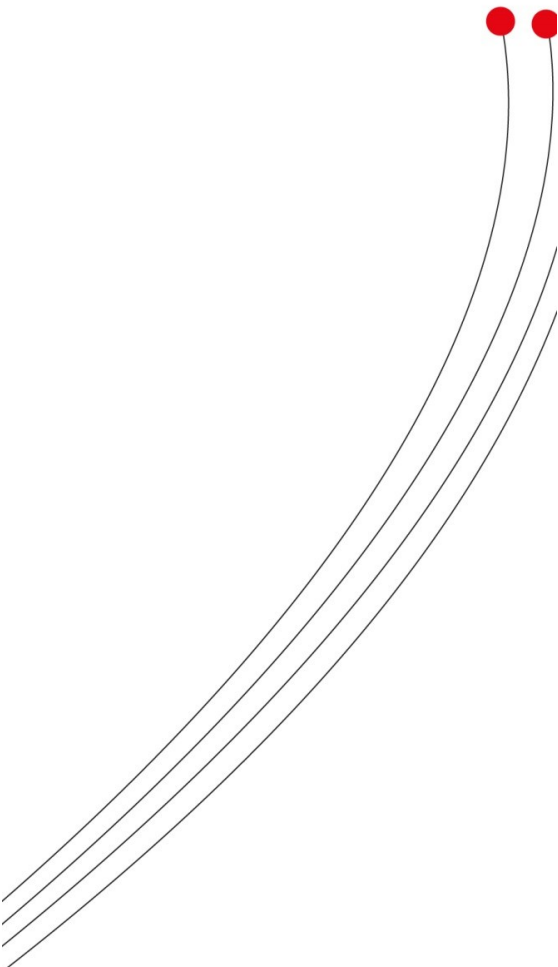


**INCENTIVES AND REPUTATION AS PREDICTORS FOR
PRIVACY CONCERNS AND PEOPLE'S WILLINGNESS TO
DISCLOSE INFORMATION TO E-VENDORS**



Sabrina Kaul
s1605275

26th of February, 2016

Incentives and Reputation as Predictors for Privacy Concerns and People's Willingness to disclose Information to E-Vendors

Master Thesis

Sabrina Kaul (s1605275)

Graduation Committee

Dr. A. Beldad

Dr. J.J. Van Hoof

University of Twente

Faculty Behavioural, Management and Social Sciences (BMS)

Program Master Communication Studies

Specialization Media and Communication

Graduation Date 26th of February, 2016, Enschede

Table of Contents

1.	Introduction	1
2.	Theoretical Framework.....	4
2.1.	Willingness to disclose personal information	4
2.2.	Privacy concerns.....	6
2.3.	Predictors	8
2.3.1.	Type of Incentive	8
2.3.2.	Corporate Reputation.....	11
2.3.3.	Personal privacy evaluation.....	14
2.3.4.	Value of incentive	15
2.3.5.	Gender as moderator	16
3.	Method.....	18
3.1.	Pretest	19
3.2.	Procedure	19
3.3.	Participants.....	20
3.4.	Manipulation	21
3.5.	Clustering of willingness to disclose.....	24
3.6.	Measures	28
3.7.	Randomization.....	28
4.	Results.....	30
4.1.	Hypotheses testing.....	30
4.2.	Further analysis	34
5.	Discussion	37
5.1.	Key findings	37
5.2.	Theoretical and practical implications	39
5.3.	Limitations and future research	41
5.4.	Take home message	43
6.	References	44
7.	Appendices	49

Abstract

Providing personal information is connected to privacy concerns and loss of control. In the domain of e-commerce an increasing demand for such information is present. The controlled use of customer data can be beneficial for both sides of the spectrum, but can also involve risks that need to be considered. Referring to the cost-benefit calculus and the privacy paradox, incentives and other predictors play a role for customers to decide on disclosure of personal information to e-vendors.

The study at hand aimed to investigate the influence of incentives and corporate reputation on privacy concerns and willingness to disclose personal information. An online survey with 369 German respondents was conducted to examine these effects using a fictional vendor website in six different conditions. In the presented scenarios the e-vendor requested their customers to reveal personal information by filling out a questionnaire. The e-vendor would compensate the customers for disclosing information with either a monetary or non-monetary reward. Three different variations for corporate reputation were used – two positive reputations with emphasis on either service performance or privacy protection, and one negative reputation.

The results revealed that willingness to disclose is influenced by the value of an offered incentive, by personal privacy evaluation, privacy concerns, and partially by corporate reputation. Furthermore, privacy concerns are only affected by value of incentive and personal privacy evaluation.

The study yielded theoretical and practical implications, such as the knowledge about the importance of the value of an incentive. A distinction between monetary and non-monetary benefits is not that relevant when choosing a reward system. Researchers and e-vendors should concentrate more on offering incentives that are valuable for the target group. A compensation that is perceived as beneficial and worthy has a stronger impact on people than a reward that is taken as indifferent. Furthermore, people who are generally concerned about their privacy are also more concerned about the protection of their privacy on websites that request information. It needs to be further investigated how privacy concerns can be lowered in general to make information disclosure more likely.

Keywords: incentive, e-commerce, information disclosure, privacy concerns, privacy evaluation, corporate reputation, value of incentive, benefits, privacy paradox, cost-benefit calculus

List of Tables

Table 1 Demographics of the respondents	21
Table 2 Mean ratings of monetary and non-monetary conditions (with SD), as well as t- and p-values for manipulation check items.....	22
Table 3 Mean ratings of positive corporate reputation - service performance and privacy protection, and negative corporate reputation (with SD) for manipulation check items	23
Table 4 Items and reliability of the sub-variables of willingness to disclose personal information	25
Table 5 Scale descriptives of the sub-variables of willingness to disclose personal information.....	26
Table 6 New hypotheses after splitting the variable willingness to disclose personal information.....	27
Table 7 Scale descriptives of the constructs used in the study.....	28
Table 8 Frequencies, percentages, mean age and gender distribution of the six conditions.....	29
Table 9 Descriptives for type of incentive, corporate reputation, and gender with regard to the dependent variables.....	31
Table 10 Multivariate analysis of covariance of the variables used in the study.....	32
Table 11 Results summary of hypotheses testing.....	34
Table 12 Multivariate analysis of variance of type of incentive, and corporate reputation.....	35
Table 13 Multivariate analysis of variance of type of incentive, corporate reputation, and gender ...	36

List of Abbreviations

CR	Corporate Reputation
MI	Monetary Incentive
MN	Monetary Incentive + Negative Reputation
MPP	Monetary Incentive + Positive Reputation – Privacy Protection
MPS	Monetary Incentive + Positive Reputation – Service Performance
N	Negative Reputation
NMI	Non-monetary Incentive
NN	Non-monetary Incentive + Negative Reputation
NPP	Non-monetary Incentive + Positive Reputation – Privacy Protection
NPS	Non-monetary Incentive + Positive Reputation – Service Performance
PC	Privacy Concerns
PP	Positive Reputation – Privacy Protection
PPE	Personal Privacy Evaluation
PS	Positive Reputation – Service Performance
Tol	Type of Incentive
Vol	Value of Incentive

1. Introduction

Online shopping has become a major research field in recent years. People got used to the idea of buying things on the Internet from anywhere at any time. Providing information about names, bank accounts and addresses is necessary to successfully finish the transaction processes. Companies may also ask for more information that is not relevant to the context, but rather assist them to individualize advertising messages. Disclosing this kind of information to e-vendors (companies that sell products and services online) can involve a certain risk. For instance, companies could sell the information to a third party or misuse the information by charging more than agreed on.

Uncertainty about the use of personal data causes people to hesitate to provide information. Son, Kim, and Riggins (2006, p. 482) describe this phenomenon as "an online shopper's perception of the possibility of having undesirable outcomes [...] because of his or her inability to monitor and evaluate the performance of online vendors". This means that asking for information is not enough. Transparency and other mechanisms need to be activated in order to achieve a balanced information exchange and to receive the necessary trust of the customer.

Disclosing information can also result in benefits for both parties, for the companies and the customers. E-vendors can improve their products on the basis of direct feedback, personalize commercial emails and enhance offers to better fit their customers' taste, or use the information to better understand their target group as a whole, which in return will be beneficial to the customers.

In the following, recent researches with focus on the reasons why people provide information despite their privacy concerns are described. One field of interest is the use of benefits to entice online shoppers to give more information than they would normally disclose. These incentives can be of monetary nature or provide other compensation for revealing personal information.

Studies focused on the interplay between offering incentives and the sensitivity of information asked for. Weible (1993, p. 30) defines information sensitivity as "the level of privacy concern an individual feels for a type of data in a specific situation". For instance, one research team discovered that when offering monetary rewards in exchange for highly sensitive information, privacy concerns of people increase. Hence, it is unlikely that the information would be provided after all (Lee, Lim, Kim, Zo, & Ciganek, 2013). The researchers explain their results by suggesting that monetary incentives are seen as a decoy and that people feel tricked into doing something they

normally would not agree to. Furthermore, they agree that monetary rewards increase and decrease privacy concerns amongst different contexts. In other words, incentives might work differently when other factors are present, for instance, depending on the kind of information that is requested, brand preferences, or reputation of the requesting institution.

Corporate reputation might influence the context, in which a person is asked to provide personal information. Depending on the standing of the company, people decide differently about engaging with the company. Eastlick, Lotz, and Warrington (2006) investigated the influence of reputation, trust, commitment and privacy concerns on the purchase intention and information choice strategy of customers. The researchers discovered that a positive corporate reputation decreases people's privacy concerns, which consequently leads to a higher purchase intention. This suggests that a positive reputation could also influence people's willingness to disclose information to e-vendors. Corporate reputation can be built upon a variety of characteristics. For instance, the company might be a leader in the field of privacy protection, or it is known for its outstanding customer service.

The study at hand provides additional data to explain factors that influence people's decision making processes. Research has been done on the different influences that the combinations of incentives and other variables have on privacy concerns and on disclosure behavior. But as stated in the following, these studies yielded inconsistent results; hence, it is of interest to further research the influence of different types of incentives and corporate reputation on disclosure behavior and privacy concerns. This study conducts an experimental research to elaborate on the following question.

“To what extent do different types of incentives and different types of corporate reputation influence people's willingness to disclose personal information to e-vendors and their privacy concerns?”

The research question demands an extended understanding of the interaction effect of type of incentive and corporate reputation. Furthermore, gender might moderate the effects of incentives and reputation. Consequently, two sub-questions can be derived and will be included in the research.

“To what extent do type of incentive and corporate reputation have a combined effect on privacy concerns and people's willingness to disclose information?”

“To what extent does gender affect the influence of type of incentives and corporate reputation on people’s willingness to disclose personal information?”

The results might be of interest for organizations, which can profit from the knowledge of how to successfully gather customers’ information to use for product and service enhancements. In addition to that, the theoretical relevance lies in the investigation of factors that affect decision-making processes in the privacy domain. More specifically, exploring the predicting influence of offering different types of incentives and benefits gained from having a positive corporate reputation on people’s choice to disclose personal information despite of privacy concerns, value of incentive and people’s general privacy evaluation.

The paper at hand elaborates first on research results relating the willingness of people to disclose personal information, and privacy concerns. This is followed by a discussion of the possible predictors such as type of incentive, corporate reputation, personal privacy evaluation, value of benefit, and gender. Method development and results are explained after that and are followed by the conclusion section. The paper closes with a discussion elaborating on references to previous research, limitations, implications, and recommendations for future research.

2. Theoretical Framework

The study at hand answers the following research question, which is derived from the inconsistent results revealed from previous research: “To what extent do different types of incentives and different types of corporate reputation influence people’s willingness to disclose personal information to e-vendors and their privacy concerns?” The theoretical framework provides a comprehensive discussion of the variables prominent in this study.

2.1. Willingness to disclose personal information

As mentioned above, e-commerce companies can use personal information given by customers to enhance their products and services, as well as optimize targeted advertising strategies in order to maximize their profits and their overall standing within the market. Detailed personal information can only be gathered by asking users to reveal it. Thus, e-vendors need to count on their customers’ willingness to disclose this kind of information, because they are the only ones who can provide it.

The willingness to disclose personal information in the study at hand is defined as the intention of an individual to freely provide personal information to a person, an organization or a website. Willingness to disclose information is the feeling to be ready to intentionally reveal information, after considering the benefits and the risks accompanying this decision. This definition was formed after considering the works of Premazzi, Castaldo, Grosso, Raman, Brudvig, and Hofacker (2010), Wakefield (2013), Yang and Wang (2009), and Li (2014).

The theory of reasoned action (Fishbein & Ajzen, 2010) and its expanded version, the theory of planned behavior (Ajzen, 1991), both state that attitude influences intention, which leads to behavior. Ajzen (1991, p. 181) states that “as a general rule, the stronger the intention to engage in a behavior, the more likely should be its performance”. Consequently, measuring the intention to behave in a specific way is reliable enough and the best way to successfully predict an individual’s behavior (Heirman, Walrave, & Ponnet, 2013). Furthermore, Wakefield (2013) points out that, based on the theory of reasoned action, people tend to provide information if they believe that a website is taking good care of the personal data in terms of security.

Privacy statements and privacy seals enhance the chance of customers to disclose information to e-vendors (Hui, Teo, & Lee, 2007). These concepts imply that users can rely on and trust in the website’s ability to ensure safety for the stored information. In agreement, Dinev and

Hart (2006) add trust to the list. Furthermore, they introduce personal Internet interest as a reason for people to reveal information. They argue that personal interest motivates people to be more willing to provide information when they need to, in order to gain access or proceed in a transaction. Hence, disclosure is a goal oriented behavior.

In addition to factors that encourage willingness to disclose information, several theories suggest that disclosure is a conscious cognitive process.

Communication privacy management (CPM) is a theory that provides an explanation to understand people's decision making about disclosing and withholding personal information. It states that the concepts of disclosure and withholding interact with each other and people apply a rule management system to deal with the tension between these conflicting poles (Petronio & Wesley, 2014). CPM is based on five assumptions – (1) People assume they own information about themselves, and because of that (2) they have the right to control the information transfer. (3) Individuals use rules to make the decision to disclose or withhold information and assume that once they share information, (4) other people will follow the same rules to handle the entrusted information. Lastly, (5) when privacy rules are violated, people experience some kind of disturbance of their communication privacy management (Petronio, 2007). This explains that people undergo some kind of decision making process when asked to reveal personal information to other individuals and companies.

Privacy calculus is an approach to explain the actual cognitive process that occurs when people are asked to disclose personal information. Culnan and Bies (2003) first refer to the term privacy calculus when discussing consumers' privacy concerns and their perceived level of fairness of privacy practices by companies. They state that individuals first perform a cost-benefit analysis before they decide to reveal personal information. Consequently, people will disclose personal information when they feel that benefits, such as monetary or non-monetary incentives outweigh their privacy concerns, perception of risk or skepticism. Blau (1986) clarifies that joy (benefits) experienced by one party, causes displeasure (costs) to others. Consequently, providing information to an e-vendor, thus helping the organization to gain knowledge and profit, might cause harm or discomfort for the person who provides the information.

Derived from the results of the mentioned studies, four factors were chosen to be predictors for people's willingness to disclose personal information and privacy concerns for this research. Type of incentive and corporate reputation have been found to separately be influencing the decision to reveal information, and perceived privacy concerns in prior studies (among others Koohikamali, Gerhart, & Mousavizadeh, 2015; O'Neil & Penrod, 2001; Taylor, Davis, & Jillapalli, 2009; Lee, Lim,

Kim, Zo, & Ciganek, 2013; Metzger, 2006; Andrade, Kaltcheva, & Weitz, 2002 ; Xie, Teo, & Wan, 2006). (1) Monetary and non-monetary incentives might influence the cost-benefit calculus in terms of trying to outweigh risks that accompanying disclosure behavior, and have an effect of the level of privacy concerns connected to the situation. (2) A positive corporate reputation in terms of service performance and privacy protection can have an influence on the perception of trustworthiness an online user holds, which would thereby affect the decision to reveal information, and the perceived concerns of privacy.

According to previous research (among others Rensel, Abbas, and Rao, 2006; Xu, Dinev, Smith, and Hart, 2011; Hann, Hui, Lee, and Png, 2007; Yang et al., 2009) personal privacy evaluation and the value of incentives are important factors that do not require manipulations, but are set personal dispositions that might influence disclosure as covariates. Furthermore, it can be assumed that more than just two factors may influence a person's decision to reveal. (1) Personal privacy evaluation describes a personal disposition to privacy and might explain why some people are more inclined to withhold information than others. (2) The value of incentive varies from person to person and thereby influences people differently. Benefits might trigger different behaviors and perceptions, according to their worth to the person.

2.2. Privacy concerns

Privacy is not a universal term that can be applied to anyone in the same manner. Privacy has different values and meanings, varying from person to person and contexts. Westin (1966) describes four states of privacy – solitude (being left alone, but part of a group), intimacy (relationship with small group or individual persons), anonymity (being an unidentifiable person in public), and reserve (holding back any kind of information). This categorization helps to explain why people might evaluate their personal privacy differently in various contexts. Connecting this knowledge to the study at hand – when shopping online or looking for information on the Internet, people might want to be anonymous and act as freely from judgement as possible. That would explain why people would not be willing to disclose personal information to e-vendors. Additionally, why concerns about safety of their privacy might increase.

Privacy concerns are the customer's perceptions about the "*inability and unwillingness*" of the vendor to secure the customer's "personal information from improper use, disclosure to third parties, and secondary use without the buyer's consent" (Pavlou, Liang, & Xue, 2007, p. 113). Improper use means that organizations, for instance, might sell the information or publish it in form

of an advertisement. This leads to the notion that privacy concerns indicate a lack of trust between customers and the organization. If the customers cannot trust the organization with their personal information, to keep them safe and protected from outside attacks, PC rise and might influence the decision to disclose personal information in the first place. Consent is another key word in that definition – customers want to have control over who can access their data and where and when this happens. Losing control over the distribution of personal data might evoke privacy concerns about the organization's intentions.

There is a difference between online privacy concern and website privacy concern (Li, 2014). Online privacy concern addresses risks and fears about privacy loss in the whole Internet landscape, whereas website privacy concern describes the consumers' perception of risks concerning a specific website. Acknowledging this difference is important, because people might have different perceptions of losing privacy on different websites. In the study at hand, the term privacy concerns will be addressed and interpreted as defined by the concept of website privacy concern, due to the fact that the participants will rate their perception of the given website example.

Research has shown that online privacy concern has no significant negative relationship with the intention to provide information, but website privacy concern does (Li, 2014). It can be stated that the less website privacy concerns an individual perceives, the more that person intends to disclose personal information. Wakefield's (2013), and Yang et al.'s (2009) studies support the assumption that privacy concerns are negatively related to the intention to provide information.

Norberg, Horne, and Horne (2007) discovered a privacy paradox. People claim to be concerned about providing information to organizations and to withhold it. When studying the actual behavior, the study by Norberg et al. (2007) found that the same people whose intention is to conceal personal information, in fact provide it willingly. The researchers explain this phenomenon by saying that perceptions of trust and risks vary in imaginary and real situations. Circumstances differ and other variables might influence the actual behavior. Consequently, the study at hand uses two manipulated variables and a number of covariates to be able to better control for the chance of a privacy paradox. For instance, the relationship between offered incentives and privacy concerns is also influenced by other factors, like value of incentive and information sensitivity (Yang et al., 2009). It needs to be considered, that factors outside of the control of organizations might be of influential impact as well; for instance, personal disposition towards privacy.

H1: People who have high privacy concerns (PC) regarding a website are less willing to disclose personal information than people who have low privacy concerns

2.3. Predictors

The independent variables in the study at hand are type of incentive and corporate reputation. Both variables will be manipulated in the research, which will try to capture the influence of different types of incentives and different types of corporate reputation on people's privacy concerns and their choice to reveal personal information to an e-vendor. Furthermore, personal privacy evaluation and value of incentive are additional factors that might have an effect on privacy concerns and people's willingness to disclose.

2.3.1. Type of Incentive

As Cicero once said, "there is no more essential duty than that of returning kindness" (Cicero and Peabody, 1887, p.32). That would mean that by offering some kind of benefit to a customer, he or she should feel the need to reimburse the company for their helpfulness. This phenomenon is called reciprocity and is a widely discussed topic in social and psychology science, primarily associated with social exchange theory.

Blau (1986, p. 4) focused on the individual level concerning the theory in the context of commerce. He states that "a person for whom another had done a service is expected to express his gratitude and return a service when the occasion arises". Gouldner (1960) agrees and adds that the reaction to an act of kindness is some kind of forced repayment. In other words, if person A gives a gift to person B, person B feels obliged to return the favor. For instance, Goranson and Berkowitz (1966) found evidence in their study about reciprocity and responsibility reactions to prior help that people, who receive help on a voluntarily basis, feel more obligated to repay the favor than people who are denied help.

The concept of distributive justice relates to reciprocity in a way that the repayment should be of equal worth to the first act of giving to keep a balance in the exchange (Schwartz, 1967; Blau, 1986). This ensures stability in a social system. It is to be investigated whether incentives offered by companies can match the value of personal information in the eyes of customers. This phenomenon will be of importance when discussing the covariate value of incentive later on.

Different types of incentives (ToIs) were offered in the study at hand in order to investigate if they stimulate reciprocity and lead to customers' willingness to disclose personal information. The term incentive has a variety of synonyms (reward, compensation, benefit, gain, value, and gift) that will be used interchangeably in this report. Incentives are "offers provided [...] to a user to encourage

a specific behavior" (Koohikamali, Gerhart, & Mousavizadeh, 2015, p. 81). Put differently and adjusted to this context, offering an additional benefit for the customer may lead to decreased privacy concerns and a stronger intention to disclose personal information, because they do not want to be in debt to the company. As mentioned before, there are two kinds of incentives to be considered: (1) monetary incentives, and (2) non-monetary incentives.

2.3.1.1. *Monetary incentives*

Monetary incentives (MI) are definite cash-equivalent rewards received in exchange for, in this case, giving personal information. These may include money, gifts or discounts.

Providing monetary compensation increases privacy concerns (Yang et al., 2009). Offering money could be seen as a decoy and distract the customer from an unwanted access to personal data. Consequently, monetary incentives may be perceived negatively.

Lee, Lim, Kim, Zo, and Ciganek's (2013) confirmed the results found by Yang et al. (2009) by researching the influence of information sensitivity on privacy concerns, disclosure of information and misrepresentation of information with monetary rewards as a moderating factor. Their research shows that MIs do not enhance the possibility of the intention of consumers to provide personal information. But they discovered that the interplay of information sensitivity and monetary rewards affects disclosure intention. The use of monetary rewards is more successful, when people are asked to provide less sensitive information. The researchers suggest that when asking for highly sensitive information, companies should strengthen people's trust rather than offering MIs.

Interestingly, Premazzi et al. (2010) found that people's willingness to disclose did not increase when offering compensation, but when testing the actual behavior, they discovered that people were disclosing personal information after all. This shows that respondents may claim to behave in a specific way in attitudinal studies, but might act differently in a real situation. This phenomenon is known as privacy paradox.

Premazzi et al. (2010) explain their results by referring to the cost-benefit calculus – people have the impression of a fair and balanced trade, when offered a compensation for providing their information. The approved consensus is that "a positive net outcome should mean that people are more likely to accept the loss of privacy that accompanies any disclosure of personal information as long as an acceptable level of risk accompanies the benefits" (Culnan & Bies, 2003, p. 327). In short, the incentives must outweigh the risks that come with disclosing personal information.

2.3.1.2. *Non-monetary incentives*

Non-monetary incentives (NMI) can take on a variety of shapes. The key aspect is that this kind of incentive has no cash-equivalent. Put differently, it is a gain for customers that cannot be returned or sold to receive money (Taylor et al., 2009). These incentives can include assistance, services, special access, personalized gifts, customization or “any other form of benefits prized by customers” (Yang et al., 2009, p. 39).

In Jeffrey and Shaffer’s (2007) framework about motivational aspects of tangible benefits a categorization system of the characteristics of incentives is introduced. The researchers differentiate between four motivations – (1) Justifiability – people would usually not get it for themselves and therefore are free to enjoy the incentive, (2) social reinforcement – striving for a reward, because it is visible to others and indicates status, (3) separability – monetary incentives are seen as part of something bigger and are therefore less valuable, for instance, a Christmas bonus is part of the monthly income, and (4) evaluability – the value of a non-monetary reward changes from person to person, this kind of motivation is more connected to an emotional evaluation of the incentive.

Most relevant for the study at hand are motivations via social reinforcement and evaluability. By offering a NMI that is not accessible to anyone, owning and using the incentive can be beneficial to one’s status in a social group and hence, increase the chance of a person to provide information. Also, it needs to be considered that not all people can be motivated by the same reward – offering an uninteresting compensation might not result in a greater willingness to disclose personal information, according to evaluability.

Hammermann and Mohnen (2014) investigated the different effects of monetary and non-monetary rewards on effort and quality of behavior in the context of tournaments. Their study shows that MIs strongly influence people to put more effort into their behavior than when enticing with NMIs. The researchers suggest that money clearly distinguishes between winners and losers of a contest, whereas NMIs might be perceived as a consolation prize or a simple sign of participation. Relating these findings to the context of the study at hand, one could say that offering monetary incentives would outperform non-monetary rewards when trying to convince people to willingly provide personal information to e-vendors, because MIs are valued higher than NMIs.

In contrast, Mahmood and Zaman (2010) experienced the complete opposite results in their study of students receiving either money or a gift in return for completing a task. The monetary reward was chosen more often, but the respondents put more effort into their work when receiving the non-monetary incentive. The researchers explain that a non-monetary incentive is seen as a

present, which represents kindness and evokes reciprocity and a feeling of being in debt, whereas monetary rewards are some kind of unemotional expense allowance, which does not trigger reciprocal behavior and raises no need to restore a balance of social exchange. That means for the study at hand that people are more willing to provide information when offered non-monetary incentives than cash-equivalent benefits.

These contrary results indicate an opportunity for further research on the influence of the different types of incentives on people's privacy concerns and their willingness to disclose personal information, which the study at hand will seize.

H2: People who are offered monetary incentives (MIs) have higher privacy concerns than people who are offered non-monetary incentives (NMIs)

H3: People who are offered monetary incentives (MIs) are more willing to disclose personal information than people who are offered non-monetary incentives (NMIs)

2.3.2. Corporate Reputation

The second independent variable, which will be manipulated in the study at hand, is corporate reputation (CR). Gotsi and Wilson (2001, p.29) give a comprehensive definition of reputation, which will be used as a frame to manipulate the different scenarios in the study at hand. Accordingly, "a corporate reputation is a stakeholder's overall evaluation of a company over time. This evaluation is based on the stakeholder's direct experiences with the company, any other form of communication and symbolism that provides information about the firm's action and/or a comparison with the actions of other leading rivals".

Reputation as perceived by customers is a strong predictor for the trust they account to the company (Jarvenpaa, Tractinsky, & Saarinen, 1999). As discussed in the section about privacy concerns, concerns regarding the protection of privacy depict a lack of trust; consequently a positive corporate reputation decreases privacy concerns.

When companies ask their customers to behave in a certain way, for instance filling out a questionnaire or buying certain products, a positive reputation can increase the chance of people complying (Newbury, 2010). In other words, customers want to be of assistance to a company with a positive corporate reputation. Hence, they are more likely to be persuaded by the organization to

behave in a firm supportive way and help out with the resources, for instance personal information, they have at their disposal.

As the definition by Gotsi et al. (2001) suggests, reputation consists of multiple aspects. To further investigate the different shapes reputation can take on and whether there is a distinct difference in levels of influence on disclosure behavior and on privacy concerns, the variable is split into three conditions; namely (1) positive corporate reputation with emphasis on service performance, (2) positive corporate reputation with emphasis on privacy protection, and (3) negative corporate reputation with emphasis on both aspects.

According to stakeholder theory (Freeman, 2010), a company should not only focus on one stakeholder, but be attractive to all stakeholders important to the company. Stakeholders hold power over the success of a company and are simultaneously influenced by it. With respect to this assumption, corporate reputation is differentiated, which may represent the address of different stakeholder groups.

Corporate reputation with an emphasis on service performance was chosen to investigate how customers derive perceptions of organizations' ability and willingness to protect customers' information from characteristics not connected to safety. The question to be answered is whether a company that is known for providing high quality services and products is also perceived as trustworthy in terms of privacy protection. In contrast, corporate reputation with an emphasis on privacy protection was chosen to observe if customers value a company's effort to protect customer data and reward it with less privacy concerns regarding its website.

2.3.2.1. Service performance

Corporate reputation with an emphasis on service performance (PS) lays the focus on achievements, power, reliability of services, and satisfaction of customers. Stakeholders should value an organization for its outstanding performance in products, goods and services in comparison to competing organizations. On the basis of these factors stakeholders can form a corporate reputation, which can influence their attitude towards the company's behaviors and requests.

Eastlick et al. (2006) examined the relationship between trust, commitment, purchase intention, reputation and privacy concerns in a B2B-environment. Their definition of reputation fits the differentiation of PS made in the study at hand. The researchers argue that reputation consist of an organization's skills and personality. The emphasis lies on size and level of success of a company and its range of products, experience, and customer-oriented behavior. Their study revealed that a

positive corporate reputation decreases privacy concerns, which would in turn increase trust in and commitment to the organization.

Metzger (2006) agrees that reputation is built on the performance a website or company showed in the past, which can be used as an indicator for predicting the likelihood of future behavior. In her study about the effects of websites, vendors and consumer characteristics on website trust and disclosure of information, reputation was the most important factor in predicting disclosure behavior. Nevertheless, the results indicate that there is no significant evidence for this influence. Hence, more research needs to be done to support her assumption.

2.3.2.2. Privacy protection

Corporate reputation with an emphasis on privacy protection (PP) lays its focus on security and safety of customers and their information. Stakeholders form a reputation on the basis on how well a company is able to secure and protect customers' data from third parties. Consequently, the impression of stakeholders is dependent on how trustworthy they perceive the organization to be.

Andrade, Kaltcheva, and Weitz (2002, p.167) argue that "developing a reputation for trustworthiness" positively influences people's cost-benefit calculus outcome towards deciding to disclose personal information. Supporting this line of thought, Xie et al. (2006) conducted a study about the influence of reputation, privacy notices and rewards on online consumer behavior and found that reputation affects people's decision to disclose personal information. That is, a PP increases the likelihood of information disclosure.

Li (2014) discovered that reputation was the better variable in his model than disposition to privacy and website familiarity to predict people's privacy concerns. Furthermore, the results indicate that websites with less favorable reputations appear to be not committed enough and do not have the necessary competencies at their disposal to ensure privacy.

H4: People who are confronted with a website with a positive corporate reputation have lower privacy concerns than people who are confronted with a negative corporate reputation

H5: People who are confronted with a website with a positive corporate reputation, privacy protection wise (PP), have lower privacy concerns than people who are confronted with a positive corporate reputation, service performance wise (PS)

H6: People who are confronted with a website with a positive corporate reputation are more willing to disclose personal information than people who are confronted with a negative corporate reputation

H7: People who are confronted with a website with a positive corporate reputation, privacy protection wise (PP), are more willing to disclose personal information than people who are confronted with a positive corporate reputation with emphasis on service performance (PS)

2.3.3. Personal privacy evaluation

Acknowledging the difference in people's evaluation of personal privacy, Westin (1991) established a categorization for people according to their level of privacy concerns. There are three types of people, which descend in their need for privacy protection from high to low – the privacy fundamentalist, the pragmatic, and the unconcerned. In addition to a varying evaluation of privacy due to context change (see privacy concerns related to a specific website), people are generally more or less likely to be concerned about the protection of their own privacy, which might influence concerns they have when acting in various contexts, for instance when being online.

Personal privacy evaluation (PPE) displays individual perceived privacy concerns a person holds in general, not based on a specific website, but on interaction with other people and organizations surrounding the person. In general, people are mostly concerned regarding four areas when it comes to disclosing personal information to a second party – collection, errors, unauthorized secondary use, and improper access (Smith, Milber & Burke, 1996).

Yao, Rice, and Wallis (2007) state that privacy concerns a person perceives in the physical world, will influence the concerns a person holds about privacy online. Consequently, PPE might influence the decision-making process of willingness to disclose personal information on the basis of privacy concerns a person attributes to a specific website.

In the study at hand privacy concerns will be measured in relation to a specific website, but PPE will be measured in general for the point in time of the survey to observe the differences of the manipulated types of incentives offered and presented corporate reputation.

Xu, Dinev, Smith, and Hart (2011) discovered that individuals with a high need to protect their privacy tend to desire more control over the information they provide and perceive disclosure as a highly risky behavior. This concludes to the notion that perceived concerns about privacy in

general according to a personal privacy evaluation leads to a higher level of privacy concerns with regard to a specific website.

H8: People who have a high concerns in general according to the personal privacy evaluation (PPE) have higher privacy concerns (PC) than people who possess low concerns according to the evaluation of their personal privacy

H9: People who have a high concerns in general according to the personal privacy evaluation (PPE) are less willing to disclose personal information than people who possess low concerns according to the evaluation of their personal privacy

2.3.4. Value of incentive

As discussed before, distributive justice (Schwartz, 1967) refers to an equal exchange of goods, for instance, information in return for some kind of compensation. Not only the type of incentive might have an influence on people's willingness to disclose personal information and privacy concerns, but the individual evaluation of meaning of the incentive might also have an impact. If the benefit is not worth the loss of control over information distribution, disclosure might be perceived as a risky behavior. The offered reward needs to depict a valuable gain in order to outweigh the risks in a cost-benefit calculus, which in turn might trigger disclosure behavior (Hann, Hui, Lee, & Png, 2007).

Hann et al. (2007) discovered in their study about information privacy concerns with focus on privacy policies and incentives that a higher valued compensation yield higher motivation to reveal information. The researchers explain that people exchange their information when the incentive outreaches a certain threshold, which is perceived to outweigh the risks accompanying disclosure behavior.

Prior research confirms that in general, compensation has an effect on privacy concerns – in one way or the other – but in contrast to the aforementioned study, Yang et al. (2009) discovered that the results did not vary between different levels of incentives. Consequently, they did not find proof for the importance of individual rating of incentives.

Hammermann et al. (2014) agree that more studies need to be conducted to find significant results about the influence of the perceived value of incentives (Vols). They were not able to successfully measure the intended worth of non-monetary incentives in their research and demand more research in this field.

H10: People who value the incentive (Vol) highly have lower privacy concerns than people who perceive a low value for the incentive

H11: People who value the incentive (Vol) highly are more willing to disclose personal information than people who perceive a low value for the incentive

2.3.5. Gender as moderator

Referring to communication privacy management (CPM), as explained earlier in this study, Petronio and Wesley (2014) state that people use a rule based system to decide whether to disclose or withhold personal information. People establish rules on the basis of five criteria, including cost-benefit ratio, context, motivations, culture, and gender (Petronio, 2002). The study at hand focuses on the aspect of gender in order to investigate a difference between men and women when disclosing personal information and perceived privacy concerns connected to a specific website. Men and women might differ in creating rules for revealing personal information and consequently, might behave differently.

Stokes, Childs, and Fuehrer (1981) discovered in their study about gender and sex roles as predicting factor for disclosure of personal and intimate information to strangers, acquaintances, and intimates that contradicting to their hypotheses men are more willing to reveal even highly sensitive information to strangers and acquaintances than women. The researchers suggest that characteristics associated with the male gender role, such as assertiveness and willingness to take risks, are necessary to be able to disclose personal information to unknown people. Fogel and Nehmad (2009) confirm that men show more risky behavior than women.

Kurt (2010) argues that there is no significant difference in perceived privacy concerns between women and men. Women are rather ambivalent about privacy and that men are not concerned about their privacy. Furthermore, women share more information than men, at least in a social networking context (Hoy & Milne, 2010). A possible explanation could be that women see sharing information on social networks as enjoyment and part of connecting with others. It is yet to be investigated if this notion can be referred in a commercial context.

Men are more likely to purchase goods and services online and are less concerned about their collected data to be sold to a third party. However, there is no direct or indirect influence of gender in privacy concerns (Yao, Rice, and Wallis, 2007).

H12: Men have less privacy concerns than women regardless of type of incentive offered

H13: Men have less privacy concerns than women regardless of presented corporate reputation

Only few researches focus on a distinction between genders when explaining the effect of incentives and resulting disclosure behavior. Chandon, Wansink, and Laurent (2000) state that there is no significant combined effect of gender and incentives on evoking a specific behavior. Lee et al. (2013) adds that there is no distinct difference in gender when investigating disclosure behavior. But Hammermann et al. (2014) claim that men perform better when enticed with monetary incentives than with non-monetary incentives. As the literature shows, more research in this field needs to be done. The study at hand will investigate the sub-question: “To what extent does gender affect the influence of incentives and corporate reputation on people’s willingness to disclose personal information?”

3. Method

For this study an experimental research design was chosen to test the hypotheses and the stated research questions. This method examines effects of manipulated material, in this case the different types of incentives and different types of corporate reputation on the willingness to disclose personal information, and privacy concerns. The tested model is shown in Figure 1. The experiment was set up as a 2x3 research design – two types of incentives and three variations in corporate reputation. In total, there were six different conditions that were presented to the respondents. Each respondent saw only one scenario and based on that he or she had to fill out a questionnaire.

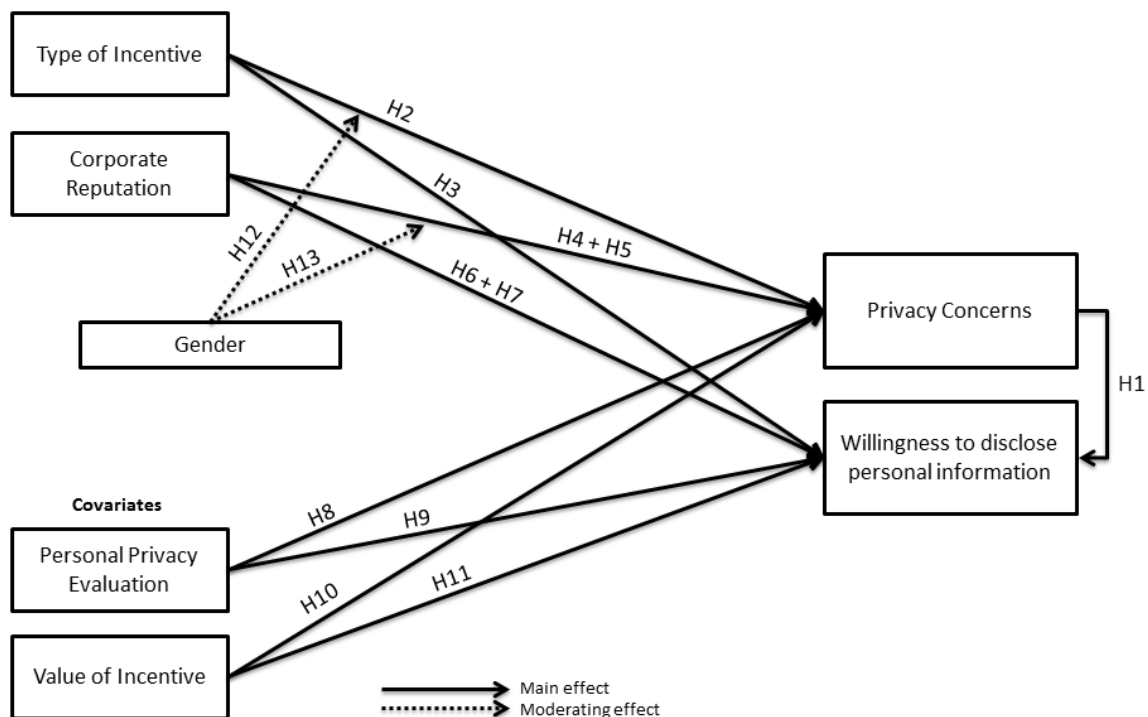


Figure 1 Tested model showing all variables and hypotheses

3.1. Pretest

Before the actual study began, the scenarios were pre-tested by 25 respondents. The participants had the chance to submit recommendations about the scenarios and were asked to indicate how often the 35 items of the shown questionnaire (presented in the scenario) have been requested of them during online shopping procedures in the past. This led to a reduction in the number of items for the actual study – from 35 to 25, consisting of the 15 most frequently requested and 10 least frequently requested items to ensure a balance of habit and novelty. The results are shown in appendix A.1.

Adjustments were made to the existing scenarios based on the recommendations and an additional literature review, which were again pre-tested in terms of their validity with 15 respondents.

3.2. Procedure

The respondents saw one of six conditions above the questionnaire they would need to fill out if they wanted to receive the presented incentive. The six combinations of type of incentive and corporate reputation are depicted in Figure 2. It was indicated that filling out the questionnaire was mandatory in order to receive the benefit, but not necessary to continue with the transaction process. The hypothetical questionnaire consisted of 25 items asking for information about identification, lifestyle, and health of the respondents.

After seeing one of the scenarios, the respondents were faced with a manipulation check to ensure the validity of their responses. In the following, the respondents were asked to indicate their level of agreement about the value of the shown reward and to what extent the incentive appealed to them.

Type of Incentive	Corporate Reputation		
	(1) Monetary + Good Corporate Reputation – Service Performance	(2) Monetary + Good Corporate Reputation – Privacy Protection	(3) Monetary + Bad Corporate Reputation
	(4) Non-Monetary + Good Corporate Reputation – Service Performance	(5) Non-Monetary + Good Corporate Reputation – Privacy Protection	(6) Non-Monetary + Bad Corporate Reputation

Figure 2 Six conditions of the combination of type of incentive and corporate reputation

The survey continued asking to what extent the respondents would have given answers to the displayed questions. They were also asked about which items evoked concerns when disclosing them.

The next two sections depicted two scales investigating the privacy concerns with regard to the presented website and personal privacy evaluation with regard to their general perception of privacy. The last part of the survey consisted of six questions about demographics and online behavior of the respondents, which helped to analyze and categorize the findings. The whole questionnaire can be seen in appendix B.

3.3. Participants

The survey was distributed through online channels and was designed for German participants exclusively. In total, 369 respondents took part in the study. Demographics and online behavior of the respondents (see Table 1) are discussed in this part to examine whether the conclusions of the research are representative for the German population.

The age of the participants ranged from 18 to 76 years. The majority of them (55.8%) are aged 20 thru 29. Women are represented with 68.6 percent, this unbalanced distribution needs to be considered when interpreting the results. Most of the respondents had obtained the highest high school degree possible in Germany (36%). 103 respondents (27.9%) possessed a bachelor's degree or an equivalent degree. Only three respondents claimed to have obtained no degree, which indicates that the sample is mainly highly educated.

Respondents with less than six years of Internet experience formed the smallest part with 4.9 percent. 205 respondents have used the Internet between six and 14 years and are the biggest group with 55.6%. Respondents, who indicated that they have 15 and more years of experience account for 39.6% of the sample.

Respondents were also asked to indicate their level of experience with online-shopping. Those who claimed to never shop online or less than once a month made up for 31.44 percent of the sample. This needs to be considered when interpreting the results, because less experience with online shopping might influence the perception of normality when being asked for personal information. 200 respondents (54.2%) claim to be in the group that shops online between one and three times a month. The smallest group consisted of 53 respondents (14.36%) whose online-shopping frequency lies between once a week and daily.

Table 1 Demographics of the respondents

Variable	Frequency	Percentage
<i>Age</i>		
• 19 years and younger	18	4.9
• 20 - 29 years	206	55.8
• 30 - 39 years	69	18.7
• 40 - 49 years	48	13.0
• 50 - 59 years	20	5.4
• 60 years and older	8	2.2
<i>Gender</i>		
• Male	116	31.4
• Female	253	68.6
<i>Education</i>		
• No degree	3	0.8
• High school degree (medium level)	9	2.4
• High school degree (high level)	133	36.0
• Apprenticeship	38	10.3
• Bachelor's degree or equivalent	103	27.9
• Master's degree or equivalent	62	16.8
• Doctoral degree	9	2.4
• Other	12	3.3
<i>Internet experience (in years)</i>		
• Up to 5 years	18	4.9
• 6 - 14 years	205	55.6
• 15 years and more	146	39.6
<i>Online-shopping experience (number of purchases)</i>		
• Never to less than once a month	116	31.4
• 1 - 3 times a month	200	54.2
• Once a week to daily	53	14.4
Total	369	100

3.4. Manipulation

The scenarios consisted of an image of a fictional commerce-website to ensure that no predetermined attributes of the company would influence the results of the manipulations.

Two different types of incentives were offered: (1) 25€ discount on next order, and (2) special access to the first three chapters of a book before the official release date and a signed copy

when the person decides to buy the book. The conditions differed in a way that one was of monetary kind and the other of non-monetary kind.

The other independent variable (corporate reputation) consisted of the following 3 variations: (1) positive corporate reputation with an emphasis on service performance, explained by good customer service and reliable shipping and return policies, (2) positive corporate reputation with an emphasis on privacy protection, explained by high compliance with national privacy regulations and a good privacy statement, and (3) negative overall corporate reputation, which is depicted with the reversed characteristics of both positive conditions. The threefold categorization of this variable was chosen, because people might perceive the strength of reputation differently based on the aforementioned characteristics. There was no distinction made between the two orientations in the negative reputation condition, because a negative reputation might always negatively influence the perception of a company, no matter the issue's origin.

In order to have a valid instrument, the different conditions of the independent variables needed to be perceived as equal. For the type of incentive an independent sample t-test showed that the mean of 4.12 for the item testing the monetary condition differed significantly from 1.62. The reversed item testing for the non-monetary condition yielded a significant difference between the mean scores of 1.64 and 4.02. The manipulation was tested on two 5-point Likert scales; the means of 4.12 and 4.02 indicated a high agreement with the intended manipulation as seen in Table 2. Hence, the manipulation of the variable type of incentive was valid.

Table 2 Mean ratings of monetary and non-monetary conditions (with SD), as well as t- and p-values for manipulation check items

	Monetary condition			Non-Monetary condition		
	Mean	<i>t</i>	<i>p</i>	Mean	<i>t</i>	<i>p</i>
I receive a 25€ voucher for filling out the presented survey ^a	4.12 (1.38)	18.377	.008	1.64(1.19)	18.377	.008
I receive access to three chapters from a book of my choice before it has been released for filling out the presented survey ^a	1.62 (1.12)	-17.305	.000	4.02 (1.52)	-17.305	.000

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

In order to prove the validity of the second independent variable, corporate reputation, an analysis of variance (ANOVA) was conducted. As one can see in Table 3, the mean scores for the overall impression of the corporate reputation only differed in 0.09 between the means of the two

positive conditions, but had a lower score on the negative condition ($N M = 1.98$ in comparison to PS 3.20 and PP 3.29). It was measured on a 5-point Likert-scale ranging from 1 = strongly disagree to 5 = strongly agree. This showed that respondents identified the manipulated material as intended in terms of the overall impression of the corporate reputation.

The negative corporate reputation condition was identified correctly in all questions with low scores under the median of 2.5 of the scales, so it can be assumed that there was a significant difference ($p < .001$) between the negative and the two positive reputation conditions.

In order to differentiate between the two positive conditions, reputations were measured with emphasis on service performance and on privacy protection. Both conditions were identified as being the positive corporate reputation. Although, when asking whether the company had a good customer service, which was connected to the service performance condition, a Bonferroni post-hoc analysis showed that there was no perceived significant difference between the two positive corporate reputation conditions.

The mean scores, the results from ANOVA, and the post-hoc analysis showed that the differences between the remaining items were significant. In sum, all manipulations were proven to be valid and added to a valid instrument.

Table 3 Mean ratings of positive corporate reputation - service performance and privacy protection, and negative corporate reputation (with SD) for manipulation check items

	PS	PP	N
Please indicate on a scale from 1 (very bad reputation) to 5 (very good reputation) your perception of the presented company ^a	3.20 (1.03) ^A	3.29 (1.00) ^A	1.98 (0.77) ^B
Weltderbücher.de has a good customer service ^a	3.50 (1.04) ^A	3.37 (1.04) ^A	2.08 (0.88) ^B
Weltderbücher.de has good shipping and return policies ^a	3.64 (1.01) ^A	3.33 (0.95) ^B	2.34 (0.92) ^C
Weltderbücher.de complies with national regulations on privacy protection ^a	2.34 (1.20) ^A	3.17 (1.40) ^B	1.64 (0.80) ^C
Weltderbücher.de has a good privacy policy ^a	2.47 (1.22) ^A	3.16 (1.38) ^B	1.66 (0.83) ^C

Notes: ^a Measured on a 5-point Likert-scale (1 = strongly disagree, 5 = strongly agree). PS = Positive corporate reputation - Service performance, PP = Positive corporate reputation - Privacy protection, N = Negative corporate reputation. ^{ABC} Conditions with a different letter code, within a row, are significantly different ($p < .05$) according to a pairwise comparison Bonferroni post-hoc analysis

3.5. Clustering of willingness to disclose

The dependent variable “willingness to disclose personal information” was split into subcategories to yield more precise conclusions about which kind of information people are willing to provide. The respondents were asked to indicate how likely it is that they would disclose the information requested in the presented scenario. Based on the results, a reliability analysis was conducted. First, all items were included in a factor analysis with Varimax rotation to see if items could be removed from the model to make it more reliable. All coefficients below .50 were suppressed. The results of this first analysis were not satisfying (see Appendix C.1). There were four items that had very weak factor loadings (below .600). Besides, one category consisted only of one item. The item Social Security Number was chosen for the study at hand after consulting American literature for inspiration. This information is not typically requested in Germany and would not yield any valuable knowledge gain. Hence, it was deleted. In order to see which other items might be deleted, multiple reliability analyses were conducted with the three remaining categories. After deleting four more items, namely blood type, gender, date and place of birth, and ethnic group – because they were weak items and did not fit the assigned groups – the dependent variable was divided into three sub-variables with 20 remaining items (see Appendix C.3). The sub-variables can be viewed in Table 5 and are called lifestyle, with a Cronbach’s alpha of .936 (10 items), identification, with a Cronbach’s alpha of .846 (5 items), and sensitive information, with a Cronbach’s alpha of .848 (5 items). The items that belong to the individual sub-variables with the corresponding factor loadings can be seen in Table 4. The names chosen for the categories correspond to the items included. Identification consisted of items related to data that can identify a specific person on the basis of the given data alone or in combination with other information. Lifestyle items were related to how people design their daily lives; and sensitive information depict items that might be the cause of discrimination. The latter category was named after reviewing article 8 of the European Union Directive on Data Protection (95/46/EC) (European Parliament & Council of the European Union, 1995), which states that data collection of this kind of information needs special care and should only be processed in exceptional cases.

Table 4 Items and reliability of the sub-variables of willingness to disclose personal information

Scales and items	Components		
	1	2	3
<i>Identification</i>			
• Address	.824		
• Name	.771		
• Email address	.760		
• Phone number	.718		
• Bank information	.631		
<i>Lifestyle</i>			
• Number of people in household		.818	
• Hobbies and interests		.791	
• Time spent online (last 7 days)		.782	
• Recent purchases online		.772	
• Type of Internet access		.769	
• Amount of cars owned		.762	
• Education		.755	
• Occupation		.747	
• Ownership or rental of home		.722	
• Product preferences		.719	
<i>Sensitive Information</i>			
• Name of health insurance company			.888
• Political party affiliation			.860
• Sexual orientation			.844
• Organ donor			.661
• Weight			.635

Notes. Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.

The respondents were asked to indicate how concerned they are about revealing certain items. Surprisingly, a factor analysis showed the same clustering as the willingness to disclose personal information construct. Deleting the same items (Social Security Number, blood type, gender, date and place of birth, and ethnic group) resulted in a clean categorization for the sub-variables (see Appendix C.2 and C.3). From this it can be concluded that the items clustered together in the willingness to disclose construct rise the same amount of privacy concerns. The scale descriptive statistics of both constructs are displayed in Table 5. The values for Cronbach's alpha are even higher than in the willingness to disclose clustering – identification $\alpha = .808$, lifestyle $\alpha = .955$, and sensitive information $\alpha = .913$.

Table 5 Scale descriptives of the sub-variables of willingness to disclose personal information

	<i>N</i>	Number of Items	Mean (SD)	α
<i>Identification</i>	369	5		
• Willingness to disclose ^a			2.73 (0.99)	.846
• Level of concern when disclosing ^b			3.09 (0.87)	.808
<i>Lifestyle</i>	369	10		
• Willingness to disclose ^a			2.00 (1.00)	.936
• Level of concern when disclosing ^b			3.25 (1.07)	.955
<i>Sensitive Information</i>	369	5		
• Willingness to disclose ^a			1.31 (0.65)	.848
• Level of concern when disclosing ^b			4.01 (1.06)	.913

Notes. ^a Measured on a 5-point Likert-scale (1 = very unlikely, 5 = very likely). ^b Measured on a 5-point Likert-scale (1 = not concerned at all, 5 = very concerned).

Due to splitting willingness to disclose into three variables, the model and hypotheses used in the study at hand needed to be adjusted. The new model can be seen in Figure 3 and the new hypotheses are displayed in Table 6.

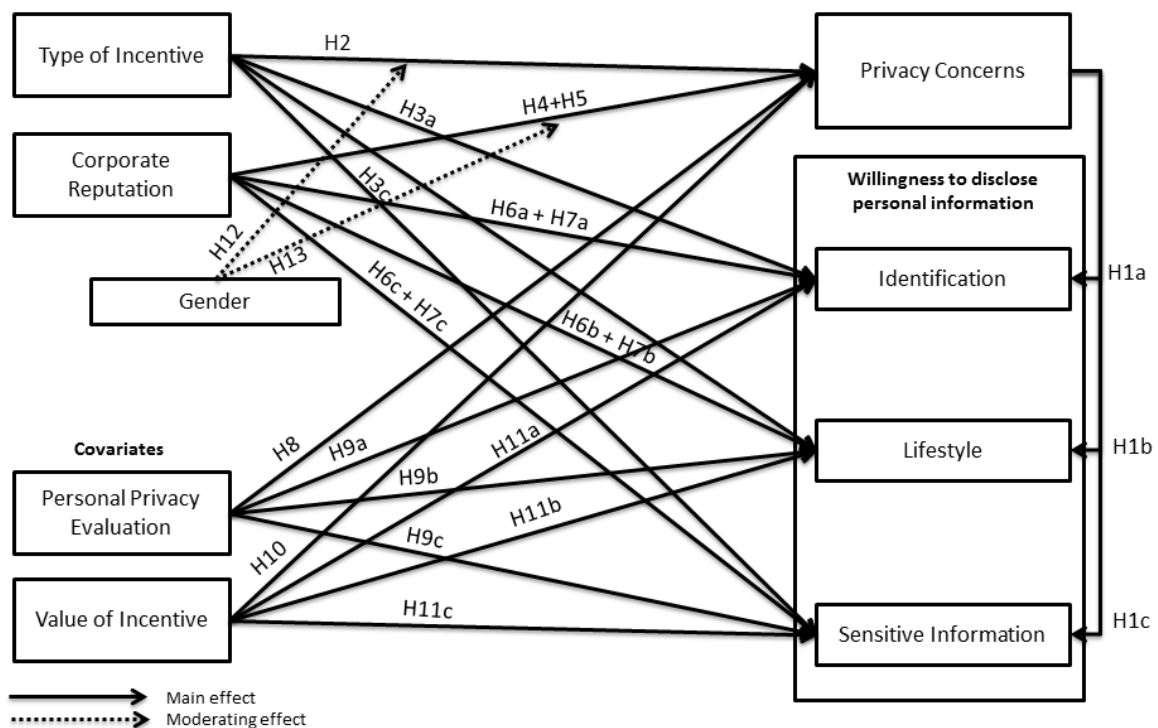
**Figure 3** Adjusted model after splitting the variable willingness to disclose personal information

Table 6 New hypotheses after splitting the variable willingness to disclose personal information

#	Hypothesis
H1	People who have high privacy concerns (PC) regarding a website are less willing to disclose a.) identification information, b.) lifestyle information, and c.) sensitive information than people who have low privacy concerns
H2	People who are offered monetary incentives (MIs) have higher privacy concerns than people who are offered non-monetary incentives (NMIs)
H3	People who are offered monetary incentives (MIs) are more willing to disclose a.) identification information, b.) lifestyle information, and c.) sensitive information than people who are offered non-monetary incentives (NMIs)
H4	People who see a website with a positive corporate reputation have lower privacy concerns than people who see the negative corporate reputation condition
H5	People who see a website with a positive corporate reputation (PP), have lower privacy concerns than people who see the positive corporate reputation (PS)
H6	People who see a website with a positive corporate reputation are more willing to disclose a.) identification information, b.) lifestyle information, and c.) sensitive information than people who see the negative corporate reputation condition
H7	People who see a website with a positive corporate reputation (PP) are more willing to disclose a.) identification information, b.) lifestyle information, and c.) sensitive information than people who see the positive corporate reputation condition (PS)
H8	People who have high concerns in general according to the personal privacy evaluation (PPE) have higher privacy concerns (PC) than people who possess low concerns according to the evaluation of their privacy
H9	People who have high concerns in general according to the personal privacy evaluation (PPE) are less willing to disclose a.) identification information, b.) lifestyle information, and c.) sensitive information than people who possess low concerns according to the evaluation of their personal privacy
H10	People who value the incentive (Vol) highly have lower privacy concerns than people who perceive a low value for the incentive
H11	People who value the incentive (Vol) highly are more willing to disclose a.) identification information, b.) lifestyle information, and c.) sensitive information than people who perceive a low value for the incentive
H12	Men have less privacy concerns than women regardless of type of incentive offered
H13	Men have less privacy concerns than women regardless of presented corporate reputation

3.6. Measures

In order to prove that the instrument consisted of reliable constructs, the covariates were tested with reliability analyses. Table 7 shows that all three variables were reliable constructs with values for Cronbach's alpha higher than .86. The value of incentive was measured with two scales, one unidimensional and one multidimensional scale. Reliability analysis indicated that both scales measure the same construct and consequently, could be recorded as one construct, consisting of 6 items and resulting in a Cronbach's alpha of .863. The scale for privacy concerns was taken from another research (Pavlou, Liang, & Xue, 2007) and yielded a reliable Cronbach's alpha of .896. Personal privacy evaluation was measured with a scale consisting of three different scales from other researches (Xu et al., 2011; Yao et al., 2007; and Beldad, 2015). Reliability analyses resulted in a three component matrix. Hence, the best working construct was chosen to be included in further analysis. The items forming the scales can be viewed in Appendix C.4.

Table 7 Scale descriptives of the constructs used in the study

	<i>N</i>	Number of Items	Mean (SD)	α
Value of incentive ^a	369	6	2.42 (1.09)	.863
Personal privacy evaluation ^b	369	3	3.56 (1.00)	.867
Privacy concerns ^b	369	6	4.22 (0.83)	.896

Notes. ^a Measured on two 5-point Likert-scales (1 = much lower, 5 = much higher, and 1 = strongly disagree, 5 = strongly agree). ^b Measured on a 5-point Likert-scale (1 = strongly disagree, 5 = strongly agree).

3.7. Randomization

The manipulated scenarios needed to be homogenously distributed among the respondents to ensure that the drawn conclusions were firm. As Table 8 shows, the six scenarios were shown to an average of 61.5 respondents. The distributions ranged from 56 to 71 participants per scenario, which was a satisfying outcome. Furthermore, the mean age in all conditions is similar. Women and men are equally distributed among the conditions. The distribution of gender is similar to the one of the whole sample; more women than men took part in the survey.

Table 8 Frequencies, percentages, mean age and gender distribution of the six conditions

Condition	Frequency	Percentage	Age <i>M</i>	Gender frequency (%)	
				Male	Female
MPS	56	15,2	32.45	20 (35.7)	36 (64.3)
MPP	71	19,2	29.34	25 (35.2)	46 (64.8)
MN	62	16,8	30.35	18 (29)	44 (71)
NPS	56	15,2	28.80	14 (25)	42 (75)
NPP	67	18,2	31.36	24 (35.8)	43 (64.2)
NN	57	15,5	32.28	15 (26.3)	42 (73.7)
Total	369	100,0	30.72	116 (31.4)	253 (68.6)

Note. MPS = Monetary Incentive + Positive Reputation – Service Performance, MPP = Monetary Incentive + Positive Reputation – Privacy Protection, MN = Monetary Incentive + Negative Reputation, NPS = Monetary Incentive + Positive Reputation – Service Performance, NPP = Non-monetary Incentive + Positive Reputation – Privacy Protection, NN = Non-monetary Incentive + Negative Reputation.

4. Results

In the following, the results of the collected data will be analyzed and interpreted. The research question “To what extent do different types (MI and NMI) of incentives and different types (PS, PP and N) of corporate reputation influence people’s willingness to disclose personal information to e-vendors and their privacy concerns?” and the stated hypotheses provided the focus for the analyses that needed to be conducted.

4.1. Hypotheses testing

For discussing the hypotheses a multivariate analysis of covariance (MANCOVA) was conducted. The descriptive statistics of the independent variables gave a first indication about whether there were main and interaction effects. MANCOVA explained whether the observed differences in mean scores were significant or not. Wilks’ Lambda values showed significant results for main effects of value of incentive ($F = 20.07, p < .001$) and personal privacy evaluation ($F = 22.72, p < .001$). The main focus of the study at hand lay on the effects of the independent variables, type of incentive and corporate reputation, which were further investigated in a test of between-subjects effects. The results can be seen in Tables 9 and 10. To compare the significant differences between the conditions of corporate reputation pairwise comparisons Bonferroni post-hoc analyses were conducted (see Appendix D.1).

Table 9 Descriptives for type of incentive, corporate reputation, and gender with regard to the dependent variables

	Mean (SD)			
	Identification ^a	Lifestyle ^a	Sensitive Information ^a	Privacy Concerns ^a
MI	2.85 (0.97)	2.09 (1.03)	1.32 (0.63)	4.23 (0.81)
NI	2.61 (1.00)	1.91 (0.96)	1.31 (0.67)	4.20 (0.85)
PS	2.84 (0.92)	2.12* (1.06)	1.31 (0.64)	4.15 (0.85)
PP	2.77 (1.03)	2.03* (0.99)	1.32 (0.60)	4.06 (0.87)
N	2.58 (1.00)	1.86* (0.93)	1.30 (0.71)	4.46 (0.70)
MPS	2.77* (0.92)	2.28 (1.09)	1.31 (0.58)	4.16 (0.81)
MPP	2.87* (0.99)	2.08 (1.01)	1.33 (0.62)	4.08 (0.89)
MN	2.89* (0.99)	1.93 (0.97)	1.31 (0.69)	4.46 (0.67)
NPS	2.90* (0.92)	1.96 (1.01)	1.31 (0.71)	4.15 (0.90)
NPP	2.67* (1.07)	1.98 (0.97)	1.31 (0.59)	4.04 (0.86)
NN	2.25* (0.90)	1.78 (0.90)	1.29 (0.74)	4.45 (0.75)
Male*MI	2.66 (1.06)	2.05 (1.05)	1.43 (0.83)	4.11 (0.93)
Male*NMI	2.74 (1.15)	2.16 (1.12)	1.52 (0.90)	4.05 (0.91)
Female*MI	2.94 (0.91)	2.11 (1.02)	1.26 (0.50)	4.29 (0.74)
Female*NMI	2.55 (0.94)	1.81 (0.87)	1.22 (0.53)	4.27 (0.82)
Male*PS	2.78 (1.11)	2.36 (1.16)	1.45 (0.75)	4.04 (0.96)
Male*PP	2.75 (1.10)	1.97 (1.02)	1.44 (0.08)	3.91 (0.95)
Male*N	2.53 (1.09)	2.03 (1.06)	1.55 (1.04)	4.39 (0.75)
Female*PS	2.86 (0.82)	2.02 (1.00)	1.25 (0.59)	4.20 (0.80)
Female*PP	2.79 (1.00)	2.07 (0.98)	1.26 (0.44)	4.14 (0.82)
Female*N	2.60 (0.97)	1.79 (0.88)	1.21 (0.51)	4.48 (0.69)

Notes. ^a Measured on a 5-point Likert-scale (1 = strongly disagree, 5 = strongly agree). MI = Monetary incentive, NMI = Non-monetary incentive, PS = Positive corporate reputation - Service performance, PP = Positive corporate reputation - Privacy protection, N = Negative corporate reputation, MPS = Monetary Incentive + Positive Reputation – Service Performance, MPP = Monetary Incentive + Positive Reputation – Privacy Protection, MN = Monetary Incentive + Negative Reputation, NPS = Monetary Incentive + Positive Reputation – Service Performance, NPP = Non-monetary Incentive + Positive Reputation – Privacy Protection, NN = Non-monetary Incentive + Negative Reputation. MANCOVA was performed to examine main and interaction effects. *p < .05. **p < .001.

Table 10 Multivariate analysis of covariance of the variables used in the study

	<i>F (p)</i>					η^2
	Identification	Lifestyle	Sensitive information	Privacy Concerns	Wilks' Lambda	
Type of incentive (MI, NMI)	0.03 (.854)	0.01 (.914)	0.75 (.388)	1.97 (.161)	0.69 (.601)	.01
Corporate Reputation (PS, PP, N)	2.13 (.145)	4.13 (.043)	0.02 (.885)	0.84 (.359)	0.21 (.086)	.04
Type of incentive*Corporate Reputation (MPS, MPP, MN, NPS, NPP, NN)	4.10 (.044)	0.86 (.355)	0.04 (.850)	0.18 (.670)	1.46 (.215)	.01
Value of incentive	6.96 (.009)	41.43 (.000)	11.91 (.001)	45.53 (.000)	20.07 (.000)	.17
Personal Privacy Evaluation	25.03 (.000)	20.17 (.000)	6.25 (.013)	59.88 (.000)	22.72 (.000)	.22
Gender*Type of incentive	3.16 (.076)	3.49 (.063)	0.22 (.640)	< 0.01 (.953)	1.60 (.174)	.02
Gender*Corporate Reputation	0.27 (.607)	2.77 (.097)	< 0.01 (.947)	0.41 (.524)	1.11 (.349)	.01
Gender*Type of Incentive*Corporate Reputation	0.14 (.709)	0.15 (.703)	0.51 (.476)	< 0.01 (.958)	0.41 (.805)	< .01

Notes. Values in bold are significant at $p < .05$. MI = Monetary incentive, NMI = Non-monetary incentive, PS = Positive corporate reputation - Service performance, PP = Positive corporate reputation - Privacy protection, N = Negative corporate reputation, MPS = Monetary Incentive + Positive Reputation – Service Performance, MPP = Monetary Incentive + Positive Reputation – Privacy Protection, MN = Monetary Incentive + Negative Reputation, NPS = Monetary Incentive + Positive Reputation – Service Performance, NPP = Non-monetary Incentive + Positive Reputation – Privacy Protection, NN = Non-monetary Incentive + Negative Reputation.

H2 was not supported. The mean scores for the dependent variable privacy concerns differ slightly between monetary incentive ($M = 4.23$) and non-monetary incentive ($M = 4.20$), but the difference is not significant ($F = 1.97$, $p = .161$). H3a, H3b and H3c were not confirmed because the differences in mean scores were not significant. Type of incentive has no effect on the disclosure of identification ($F = 0.03$, $p = .854$), lifestyle ($F = 0.01$, $p = .914$), and sensitive information ($F = 0.75$, $p = .388$).

H4 and H5 were not supported. Although the mean scores between PS ($M = 4.15$) and N ($M = 4.46$) differed in terms of levels of privacy concerns, a post-hoc analysis yielded that the difference was not significant ($F = 0.84$, $p = .359$). The same applied to the mean scores between PP ($M = 4.06$) and N ($M = 4.46$), as well as the difference between PP ($M = 4.06$) and PS ($M = 4.15$). A pairwise comparison Bonferroni post-hoc analysis was conducted to investigate the significant difference between the three conditions of corporate reputation.

H6a, H6c, H7a and H7c were not supported. Corporate reputation had no significant effect on the disclosure of identification ($F = 2.13$, $p = .145$) and sensitive information ($F = 0.02$, $p = .885$) in any corporate reputation condition. But it had an effect on the disclosure of lifestyle ($F = 4.13$, $p =$

.043). Hence, H6b and H7b were supported. The difference of 0.26 (PS vs N), as well as the difference between PP ($M = 2.03$) and N ($M = 1.86$) were significant. The same applied to the mean difference of 0.09 between PP and PS.

H8 was supported. Personal privacy evaluation had an effect on privacy concerns. The MANCOVA showed that the influence of personal privacy evaluation on privacy concerns is significant ($F = 59.88, p < .001$). To further investigate the nature of the influence a regression analysis (see Appendix E.1) was performed. The analysis resulted in a positive relationship between the two variables ($\beta = .36, p < .001$). Hence, when people's concerns in general are high, their concerns for privacy protection on a specific website also rise. H9a, H9b and H9c were supported, because personal privacy evaluation had significant effects on the disclosure of identification ($F = 25.03, p < .001$), lifestyle ($F = 20.17, p < .001$), and sensitive information ($F = 6.25, p = .013$). Again, the results of the regression analysis yielded a clarification about the relationship. Personal privacy evaluation had a negative influence on the disclosure of identification ($\beta = -.21, p < .001$), lifestyle ($\beta = -.21, p = .001$), and sensitive information ($\beta = -.13, p = .011$); meaning the higher the privacy concerns in general the less likely it is for people to disclose information.

The effect of value of incentive on privacy concerns was significant ($F = 45.53, p < .001$). The nature of the relationship was identified by consulting the conducted regression analysis. The value of incentive has a negative influence on privacy concerns ($\beta = -.29, p < .001$). Consequently, H10 was supported. The value of incentive had also effects on willingness to disclose personal information. The observed differences were significant for the disclosure of identification ($F = 6.96, p = .009$), lifestyle ($F = 41.43, p < .001$), and sensitive information ($F = 11.91, p = .001$). More insights about the relationship were drawn from the regression analysis. Value of incentive positively influenced the disclosure of identification ($\beta = .17, p = .001$), lifestyle ($\beta = .32, p < .001$), and sensitive information ($\beta = .17, p = .001$), thus H11a, H11b and H11c were supported.

H12 was not supported, because there was no interaction effect of gender and type of incentive on privacy concerns. The observed differences were far from the significance level α (.05) with $F < 0.01$ and $p = .953$. There was also no interaction effect of gender and corporate reputation on privacy concerns ($F = 0.41, p = .524$) due to insufficient significance. Hence, H13 was not supported.

In order to test hypothesis 1, a regression analysis needed to be conducted. The results in appendix E.2 indicated negative relationships between privacy concerns and the disclosure of identification ($\beta = -.19$), lifestyle ($\beta = -.31$), and sensitive information ($\beta = -.24$). All p -values lay under significance ($p = .001$). H1 was supported.

A summary of the results of the hypotheses testing can be seen in table 13, it is also indicated which analysis methods were used.

Table 11 Results summary of hypotheses testing

Hypothesis	Analysis Method	Result
H1a/b/c: Privacy concerns --> willingness to disclose	Regression analysis	Supported
H2: Type of incentive --> privacy concerns	MANCOVA	Not supported
H3a/b/c: Type of incentive --> willingness to disclose	MANCOVA	Not supported
H4: Corporate reputation --> privacy concerns	MANCOVA	Not supported
H5: Corporate reputation --> privacy concerns	MANCOVA	Not supported
H6a/b/c: Corporate reputation --> willingness to disclose	MANCOVA	Partially supported *
H7a/b/c: Corporate reputation --> willingness to disclose	MANCOVA	Partially supported **
H8: Personal privacy evaluation --> privacy concerns	MANCOVA	Supported
H9a/b/c: Personal privacy evaluation --> willingness to disclose	MANCOVA	Not supported
H10: Value of incentive --> privacy concerns	MANCOVA	Supported
H11a/b/c: Value of incentive --> willingness to disclose	MANCOVA	Supported
H12: Gender*type of incentive --> privacy concerns	MANCOVA	Not supported
H13: Gender*corporate reputation --> privacy concerns	MANCOVA	Not supported

Notes. *H6b was confirmed. ** H7b was confirmed.

4.2. Further analysis

The types of incentive and the different forms of corporate reputation had an interaction effect on the willingness to disclose identification information ($F = 4.10$, $p = .044$). People who were offered non-monetary incentives when confronted with a company with PS ($M = 2.90$) were more willing to disclose identification information than people who saw the other manipulated conditions ($M = 2.77, 2.87, 2.89, 2.67, 2.25$). This result was significant, as the p -value ($p = .044$) lay under the significance level α (.05). The other observed differences in mean scores among the disclosure of lifestyle ($F = 0.86$, $p = .355$), sensitive information ($F = 0.04$, $p = .850$), and privacy concerns ($F = 0.18$, $p = .670$) were not significant.

There is no interaction effect of gender and type of incentive on the disclosure of the different types of information, although the observed differences were close to the significance level α (.05). Two of the p -values lay slightly above it, nevertheless there was no effect of gender and type of incentive on the disclosure of identification ($F = 3.16$, $p = .076$), lifestyle ($F = 3.49$, $p = .063$), and sensitive information ($F = 0.22$, $p = .640$). Furthermore, there was no interaction effect of gender and

corporate reputation on the disclosure of identification ($F = 0.27, p = .607$), lifestyle ($F = 2.77, p = .097$), and sensitive information ($F < 0.01, p = .947$).

There was also no interaction effect of gender, type of incentive, and corporate reputation. Differences for the disclosure of identification ($F = 0.14, p = .709$), lifestyle ($F = 0.15, p = .703$), sensitive information ($F = 0.51, p = .476$), and privacy concerns ($F < 0.01, p = .958$) were not significant.

After running a MANCOVA, to see the effects of all variables included in the study, two MANOVAS were conducted. The results of the MANOVAS emphasize the importance of including covariates for possible other explanations for effects observed on the dependent variables. The first one was used to see if the manipulated variables, type of incentive, and corporate reputation, had an effect on the dependent variables without the influence of covariates and moderators (see table 12). The results showed that indeed, type of incentive had a significant main effect on willingness to disclose identification information ($F = 5.50, p = .020$). A marginal significant effect of type of incentive on lifestyle information was also observed ($F = 3.30, p = .070$). Corporate Reputation had a significant effect on privacy concerns ($F = 7.91, p < .001$), when ignoring covariates and moderators. A significant interaction effect was also detected; the presence of a type of incentive and corporate reputation had an effect on the willingness to disclose identification information ($F = 4.53, p = .011$).

Table 12 Multivariate analysis of variance of type of incentive, and corporate reputation

	F (p)					η^2
	Identification	Lifestyle	Sensitive information	Privacy Concerns	Wilks' Lambda	
Type of incentive (MI, NMI)	5.50 (.020)	3.30 (.070)	0.02 (.893)	0.06 (0.815)	2.31 (.057)	.03
Corporate Reputation (PS, PP, N)	2.41 (.091)	2.16 (.116)	0.03 (.972)	7.91 (.000)	2.67 (.007)	.03
Type of incentive*Corporate Reputation (MPS, MPP, MN, NPS, NPP, NN)	4.53 (.011)	0.45 (.635)	0.01 (.992)	0.02 (.978)	1.53 (.144)	.02

Notes. MI = Monetary incentive, NMI = Non-monetary incentive, PS = Positive corporate reputation - Service performance, PP = Positive corporate reputation - Privacy protection, N = Negative corporate reputation, MPS = Monetary Incentive + Positive Reputation – Service Performance, MPP = Monetary Incentive + Positive Reputation – Privacy Protection, MN = Monetary Incentive + Negative Reputation, NPS = Monetary Incentive + Positive Reputation – Service Performance, NPP = Non-monetary Incentive + Positive Reputation – Privacy Protection, NN = Non-monetary Incentive + Negative Reputation.

The second MANOVA included the moderator gender, next to type of incentive and corporate reputation (see table 13). The results showed that corporate reputation had a main effect on privacy concerns ($F = 6.99, p = .001$). A significant interaction effect of type of incentive and

corporate reputation on identification ($F = 3.15, p = .044$) was also present. The interaction of gender and type of incentive yielded a significant effect on identification ($F = 4.76, p = .030$) and lifestyle ($F = 4.11, p = .043$). No interaction effects of gender and corporate reputation, or gender, type of incentive, and corporate reputation were found. Again, these analyses were only conducted to highlight the importance of additional factors that need to be considered next to the variables chosen for manipulation.

Table 13 Multivariate analysis of variance of type of incentive, corporate reputation, and gender

	F (p)					η^2
	Identification	Lifestyle	Sensitive information	Privacy Concerns	Wilks' Lambda	
Type of incentive (MI, NMI)	1.69 (.195)	0.53 (.467)	0.18 (.670)	0.23 (.631)	0.87 (.481)	.01
Corporate Reputation (PS, PP, N)	2.19 (.114)	2.04 (.131)	0.09 (.916)	6.99 (.001)	2.79 (.005)	.03
Type of incentive*Corporate Reputation (MPS, MPP, MN, NPS, NPP, NN)	3.15 (.044)	0.13 (.881)	0.10 (.902)	0.03 (.971)	0.96 (.464)	.01
Gender*Type of incentive	4.76 (.030)	4.11 (.043)	0.99 (.321)	0.13 (.723)	1.90 (.110)	.02
Gender*Corporate Reputation	0.01 (.986)	1.52 (.221)	0.52 (.594)	0.18 (.835)	0.74 (.654)	.01
Gender*Type of Incentive*Corporate Reputation	0.26 (.772)	0.49 (.611)	0.45 (.637)	0.56 (.573)	0.43 (.902)	< .01

Notes. MI = Monetary incentive, NMI = Non-monetary incentive, PS = Positive corporate reputation - Service performance, PP = Positive corporate reputation - Privacy protection, N = Negative corporate reputation, MPS = Monetary Incentive + Positive Reputation – Service Performance, MPP = Monetary Incentive + Positive Reputation – Privacy Protection, MN = Monetary Incentive + Negative Reputation, NPS = Monetary Incentive + Positive Reputation – Service Performance, NPP = Non-monetary Incentive + Positive Reputation – Privacy Protection, NN = Non-monetary Incentive + Negative Reputation.

5. Discussion

The study at hand was conducted to examine the effects of type of incentive, corporate reputation, value of incentive, and personal privacy evaluation on people's privacy concerns and their willingness to disclose personal information to e-vendors. Furthermore, privacy concerns' impact on people's willingness to disclose personal information was researched. In the following, key findings of the study, theoretical and practical implications, as well as limitations and suggestions for future research will be discussed.

5.1. Key findings

In the following, seven academic findings derived from the study's results are discussed and connected to the findings of prior research in the field.

- (1) In the study at hand a negative relationship between privacy concerns and the willingness to disclose personal information was found. People are less likely to provide personal information when they perceive concerns regarding the protection of their privacy. As identified by Wang, Yeh, and Jiang (2006), privacy and safety are among the most influencing factors for customers to decide on an e-vendor. This notion can be transferred to disclosure behavior towards an organization. When shopping online, bank information, name, and addresses need to be provided. That requires that the e-vendor ensures safety for the collected data and promises to honor their customers' privacy. This level of trust, and thereby lack of privacy concerns needs to be present in people when disclosing personal information of any kind to an e-vendor.
- (2) There is no influence of the type of incentive on perceived privacy concerns connected to a website, nor is there an effect on the willingness of people to disclose personal information. Neither the presence of a monetary reward nor of a non-monetary reward evoked a significant difference in intention to provide information. These findings are consistent with the results of previous studies (for instance, Lee et al., 2013). A possible reason for that might be that people perceive the presented incentive in the study not valuable enough to have a significant impact on their decision making. As noted later, the value of an incentive is an important predictor for disclosure behavior and perceived privacy concerns. Another explanation might be that the two types of incentives evoke no different perception of worth; meaning that monetary rewards are not perceived more valuable than non-monetary benefits.

- (3) A corporate's reputation has no effect on people's privacy concerns. People have privacy concerns connected to a specific website regardless of the standing of the organization. This might be due to scandals of online-organizations in the past that led to a general mistrust of people in organizations' intentions to properly secure customers' information. The findings are in line with results from Metzger (2006), but stand in contrast to what Li (2014) and Eastlick et al. (2006) discovered. The reputation of an organization has no effect on the willingness to disclose identification and sensitive information, but on providing lifestyle information. An organization that emphasizes on service performance has the highest chances to get people to provide lifestyle information. In general, a positive corporate reputation yields a higher chance on disclosure of this type of information than a negative corporate reputation. Lifestyle information might not be seen as highly sensitive information. People cannot directly be identified by it or discriminated on the basis of it. Organizations, which are known for their service performance, might be more likely to be able to use the given information to actually improve their products and services; whereas a company known for privacy protection would just store the information safely, but be perceived as not making use of the trusted data.
- (4) Non-monetary incentives are most effective when combined with a positive corporate reputation with an emphasis on service performance when trying to trigger disclosure behavior for identification information. Surprisingly, all combination scored high for identification disclosure. The lowest mean score was observed for non-monetary incentive in combination with a negative corporate reputation, which was expected. A negative reputation was anticipated to score low, because people would not engage with companies that they do not value highly. The same would apply for disclosing personal information to those organizations. These results might be due to the fact that identification information is always requested when ordering online. People might not perceive it as an extended effort to reveal this kind of information, because the organization already possesses it.
- (5) People who value their privacy in general, also have higher privacy concerns when confronted with a website that requests information from them. Also, people who value their privacy in general are less likely to disclose personal information than people who are less concerned about their privacy in general. These findings are in line with the results discovered by Xu et al. (2011).
- (6) People who value the offered incentive highly are less concerned about their privacy regarding the organization's website. This supports the theory about cost-benefit calculus. The perceived value of an incentive outweighs the risks associated with the website. Furthermore, a highly valued incentive triggers people to disclose more information among all three categories than

people who perceive the offered reward as less worthy. This confirms what Yang et al. (2009) discovered in their study – different levels of compensation lead to varying perceptions for privacy concerns and willingness to provide information.

- (7) No significant evidence was found that gender has a moderating influence on either the type of offered incentive, corporate reputation, or the combination of both. These results are in line with knowledge gained from previous research (Chandon et al., 2000).

5.2. Theoretical and practical implications

From the results, two kinds of implications can be derived – theoretical and practical. First theoretical conclusions are discussed, four aspects were identified.

First of all, there is an important knowledge gain about the importance of the perceived value of incentives offered to people. It indicates that people do not perceive incentives equally, but that they make distinctions between rewards that are actually beneficial to them and those that are not. Money, for instance, might be seen as valuable for everyone, but it might be of more worth to a person who has less money in general. Offering a book to a person who does not like to read would have no impact as an incentive. This knowledge adds to the cost-benefit calculus theory. The risk of losing control over personal information needs to be compensated by an appropriate reward in return. This reward cannot be chosen generically for all people targeted to participate in a research, but must be customized to specific interests to yield significant results. For instance, this could be done by giving respondents a choice for a reward by presenting a list of benefits to choose from.

Second, privacy concerns perceived in general are strongly related to privacy concerns associated with a specific website. Although a website might indicate special statements about how safe it is and how well it protects users' data, people who are highly concerned about their privacy in general will not be convinced by that. This assumption supports Yao et al.'s (2007) findings and implies that general privacy concerns have a strong impact on the perception of threats to privacy in other domains, for instance online-shopping, information search, or choosing service partners.

This leads to a third implication of the findings; it needs to be further investigated how privacy concerns can be lowered in general, or at least how they can be perceived as less dominant, to make information disclosure more likely. There must be some kind of mechanism, a trigger of some sort that evokes people to provide information. People, who shop online, need to reveal identification information in order to proceed in the transaction process. What does people influence

to do so and how can this be transferred to the disclosure of other kinds of information to be beneficial to e-vendors?

It was found that Germans are skeptical in general about the safety of their information and are not influenced easily by rewards or reputation of the organizations. Apparently, a deeper mechanism must be identified to prevent privacy concerns from rising and to provide a way to ensure information disclosure.

The findings of the study at hand are not only of interest for the theoretical understanding of human behavior, but also for e-vendors in their daily activities. Practical implications were identified and are discussed in the following.

It was found that the value of incentives play an important role in influencing people to disclose personal information. E-vendors should concentrate on offering specific benefits customized to their customers rather than offering a generic form of incentive that would suit the majority of people, but would not yield the desired outcome. By providing a variety of rewards to new customers to choose from, or by using cookies and recent purchase histories to target regular customers, a more sophisticated reward system could help to evoke information disclosure.

But e-vendors need to be aware that not all customers can be reached and persuaded to provide information. According to Westin (1991) the population is categorized into three levels with regard to their general privacy concerns. The results of the study at hand lead to an assumption that the majority of Germans belong to the group of privacy fundamentalists, who are very concerned and protective of their privacy. Offering rewards and emphasizing on a positive corporate reputation do not affect them. Consequently, a cost-benefit calculus is not present and cannot be influenced in any way by the organization. In agreement with Awad and Krishnan (2006), it can be suggested that e-vendors should focus on those who belong to the other two groups identified by Westin (1991) and make use of the aforementioned reward system. Organizations need to earn the trust of the general population and time will tell if people will let their guards down to make information collection possible.

Laws can play an important role in making organizations more trustworthy. If organizations have to protect their customers' data by law, people might start trusting organizations again. The European Union Directive on Data Protection (95/46/EC) is a document stating to what extent and how personal data needs to be legally processed. Processing in this context includes data collection, storage, use, and transfer, among other ways to handle data (European Parliament & Council of the European Union, 1995). Through the directive, protection of personal data should be ensured. The

question remains whether organizations comply and to what extent people are aware of the regulations that promise to protect their privacy.

Another way to earn customers' trust is a model introduced by Spiekermann and Novotny (2015). They suggest a four market system to ensure privacy for customers. Their model makes use of a separation of customers and their personal information. In one of the four markets analysts have access to anonymized data to predict future trends. In other words, customers are able to provide personal information to one website without the fear of their data being exposed, because their information will be transferred to a different platform, where all ties to them will be broken. Consequently, people can disclose information without interfering privacy concerns and e-vendors receive valuable information about their target group without losing their customers' trust.

Another issue to be considered is the ethical aspect about collecting personal data. Mason (1986) refers to four categories connected to data collection: Privacy – Accuracy – Property – Accessibility. According to this framework, personal data are property of the individuals whom they hold information over. It follows that unauthorized access by e-vendors would be highly immoral, because it would be theft – equally illegal as stealing products from a physical store.

The accessibility issue can be viewed from two sides – (1) e-vendors want to gain access to customers' information. But why are e-vendors entitled to access personal data of customers in the first place? It can be argued that e-vendors have no right to obtain information and should not use them for maximizing their profit, because this would mean exploitation for the customers. Others might argue that by gaining more insights about customers' needs and preferences, organizations can produce products and adjust services so that customers benefit from it. A second view on accessibility refers to personal data as option of payment. (2) Customers pay with their personal information in order to gain access to special content or receive discounts. This would mean that people who have less money to spend are pushed to neglect their privacy concerns and disclose personal information. They would basically sell their data to organizations in order to stay in conformity with society's standards. This notion refers to the digital divide, which describes the increasing social inequality due to lack of access to digital media and the accompanying benefits.

5.3. Limitations and future research

The findings resulting from the study at hand need to be considered with regard to some limitations. Only German participants were considered in the study. A majority of the respondents were women. Therefore, the results cannot be transferred to the general population of Germany

without taking the imbalance of gender into account. When repeating the study, a more balanced distribution should be the aim, and cultural difference could provide more insights on the topic.

Furthermore, the named sources, which were used to indicate the level of corporate reputation in the scenarios, were chosen on the basis of circulation numbers and prestige. Different sources might cause different results in credibility perception. For the future, other sources than newspapers and research institutes can be considered. Blog posts, recommendations by family members, friends or acquaintances, and customer reviews might have different impacts on the respondents.

Asking for detailed information in a survey about privacy concerns at the end of the questionnaire was perceived as misleading for some respondents. After being exposed to risky scenarios, the willingness of the respondents to provide information about themselves might be compromised. A better way to collect more valid responses and decrease confusion about the intentions of the researchers would be to ask for demographic and other information before the start of the actual questionnaire.

The results of the study showed that the value of the offered incentive has a big influence on the willingness to disclose information and the perceived privacy concerns. In the study at hand, the type of incentive used, for instance access to a book, might not be an attractive reward for every respondent. Hence, it would be of interest to incorporate a mechanism that would offer a desirable reward individualized to the respondent. This would control for perceived differences in worth of the incentives and might yield other results.

As identified by Norberg et al. (2007) measuring people's intention to behave in a specific way does not prove that they will actually behave that way. Although Ajzen (1991) claims that intention is the best predictor for behavior, which influenced the study at hand, future research should focus on investigating the actual behavior of people in order to predict people's decisions more precisely; provided that there is sufficient funding for offering appropriate incentives.

5.4. Take home message

- People are less likely to provide personal information when they perceive privacy concerns
- There is no influence of the type of incentive on privacy concerns or willingness to disclose
- Corporate reputation has no influence on privacy concerns
- Corporate reputation has no effect on people's willingness to disclose identification and sensitive information
- Corporate reputation affects people's choice to provide lifestyle information
- People are more willing to provide identification information than lifestyle and sensitive information
- People who are generally concerned about their privacy are also concerned when confronted with a website requesting information
- People who perceive the offered incentive as valuable have less privacy concerns
- Gender does not affect type of incentive, corporate reputation or the combination of both in their influence on privacy concerns and willingness to disclose personal information

6. References

- 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07).
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. doi:10.1016/0749-5978(91)90020-T
- Andrade, E. B., Kaltcheva, V., & Weitz, B. (2002). Self-disclosure on the web: The impact of privacy policy, reward, and company reputation. In S. M. Broniarczyk & K. Nakamoto (Eds.), *Advances in consumer research*. *Advances in consumer research* (Vol. 29, pp. 350–353). Valdosta (GA): Association for Consumer Research.
- Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, 30(1), 13–28.
- Beldad, A. D. (2015). Sharing to be sociable, posting to be popular: Factors influencing non-static personal information disclosure on Facebook among young Dutch users. *International Journal of Web Based Communities*, 11(3/4), 357. doi:10.1504/IJWBC.2015.072132
- Blau, P. M. (1986). *Exchange and power in social life*. New Brunswick (U.S.A.): Transaction Books.
- Braithwaite, D. O., & Schrod, P. (Eds.). (2014). *Engaging Theories in Interpersonal Communication: Multiple Perspectives* (2nd ed.): SAGE Publications. Retrieved from https://books.google.nl/books?id=K_vKBAAQBAJ
- Broniarczyk, S. M., & Nakamoto, K. (Eds.). (2002). *Advances in consumer research*. *Advances in consumer research*. Valdosta (GA): Association for Consumer Research.
- Chandon, P., Wansink, B., & Laurent, G. (2000). A benefit congruency framework of sales promotion effectiveness. *Journal of Marketing*, 64(4), 65–81. doi:10.1509/jmkg.64.4.65.18071
- Cicero, M. T., & Peabody, A. P. (1887). *Ethical writings of Cicero: De officiis, De senectute, De amicitia, Scipio's dream*. Boston: Little, Brown, and company.
- Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, 59(2), 323–342. doi:10.1111/1540-4560.00067
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61–80. doi:10.1287/isre.1060.0080
- Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online b-to-c relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, 59(8), 877–886. doi:10.1016/j.jbusres.2006.02.006

European Parliament, & Council of the European Union (Eds.). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities: Vol. 38.

Fishbein, M., & Ajzen, I. (2010). Predicting and changing behavior: The reasoned action approach. New York: Taylor and Francis Group, LLC.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25(1), 153–160. doi:10.1016/j.chb.2008.08.006

Freeman, R. E. (2010). Strategic management: A stakeholder approach. Cambridge: Cambridge University Press.

Goranson, R. E., & Berkowitz, L. (1966). Reciprocity and responsibility reactions to prior help. *Journal of Personality and Social Psychology*, 3(2), 227–232. doi:10.1037/h0022895

Gotsi, M., & Wilson, A. M. (2001). Corporate reputation: Seeking a definition. *Corporate Communications: An International Journal*, 6(1), 24–30. doi:10.1108/13563280110381189

Gouldner, A. W. (1960). The norm of reciprocity: A preliminary statement. *American Sociological Review*, 25(2), 161–178. Retrieved from <http://www.jstor.org/stable/2092623>

Hammermann, A., & Mohnen, A. (2014). The price of hard work. *Journal of Economic Psychology*, 43, 1–15. doi:10.1016/j.joep.2014.04.003

Hann, I.-h., Hui, K.-L., Lee, S.-y., & Png, I. Analyzing online information privacy concerns: An information processing theory approach. In 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07) (pp. 210b).

Heirman, W., Walrave, M., & Ponnet, K. (2013). Predicting adolescents' disclosure of personal information in exchange for commercial incentives: an application of an extended theory of planned behavior. *Cyberpsychology, behavior and social networking*, 16(2), 81–87. doi:10.1089/cyber.2012.0041

Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult facebook users. *Journal of Interactive Advertising*, 10(2), 28–45. doi:10.1080/15252019.2010.10722168

Hui, K.-L., Teo, H. H., & Lee, S.-Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly*, 31(1), 19–33.

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer trust in an internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication*, 5(2), 0. doi:10.1111/j.1083-6101.1999.tb00337.x

- Jeffrey, S. A., & Shaffer, V. (2007). The motivational properties of tangible incentives. *Compensation & Benefits Review*, 39(3), 44–50. doi:10.1177/0886368707302528
- Koohikamali, M., Gerhart, N., & Mousavizadeh, M. (2015). Location disclosure on LB-SNAs: The role of incentives on sharing behavior. *Decision Support Systems*, 71, 78–87.
- Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, 25(2), 109–125. doi:10.1057/jit.2010.6
- Kurt, M. (2010). Determination of in internet privacy behaviours of students. *Procedia - Social and Behavioral Sciences*, 9, 1244–1250. doi:10.1016/j.sbspro.2010.12.314
- Lee, H., Lim, D., Kim, H., Zo, H., & Ciganeck, A. P. (2013). Compensation paradox: the influence of monetary rewards on user behaviour. *Behaviour & Information Technology*, 34(1), 45–56. doi:10.1080/0144929X.2013.805244
- Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems*, 57, 343–354. doi:10.1016/j.dss.2013.09.018
- Mahmood, S., & Zaman, A. (2010). Monetary and non-monetary gift exchange. *The Pakistan Development Review*, 49(4 Part II), 719–740.
- Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly*, 10(1), 5. doi:10.2307/248873
- Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on web site trust and disclosure. *Communication Research*, 33(3), 155–179. doi:10.1177/0093650206287076
- Newbury, W. (2010). Reputation and supportive behavior: Moderating impacts of foreignness, industry and local exposure. *Corporate Reputation Review*, 12(4), 388–405. doi:10.1057/crr.2009.27
- 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. doi:10.1111/j.1745-6606.2006.00070.x
- O'Neil, K. M., & Penrod, S. D. (2001). Methodological variables in web-based research that may affect results: Sample type, monetary incentives, and personal information. *Behavior Research Methods, Instruments, & Computers*, 33(2), 226–233. doi:10.3758/BF03195369
- Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: a principal- agent perspective. *MIS Q*, 31(1), 105–136.
- Petronio, S., & Durham, W. T. (2014). Communication privacy management theory: Significance for interpersonal communication. In D. O. Braithwaite & P. Schrodtt (Eds.), *Engaging*

Theories in Interpersonal Communication: Multiple Perspectives (2nd ed., pp. 335–347). SAGE Publications.

Petronio, S. (2007). Translational research endeavors and the practices of communication privacy management. *Journal of Applied Communication Research*, 35(3), 218–222. doi:10.1080/00909880701422443

Petronio, S. S. (2002). *Boundaries of privacy: Dialectics of disclosure*. SUNY series in communication studies. Albany: State University of New York Press.

Premazzi, K., Castaldo, S., Grosso, M., Raman, P., Brudvig, S., & Hofacker, C. F. (2010). Customer information sharing with e-vendors: The roles of incentives and trust. *International Journal of Electronic Commerce*, 14(3), 63–91. doi:10.2753/JEC1086-4415140304

Schwartz, B. (1967). The social psychology of the gift. *American Journal of Sociology*, 73(1), 1–11. Retrieved from <http://www.jstor.org/stable/2776124>

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2), 167. doi:10.2307/249477

Son, J., Kim, S. S., & Riggins, F. J. (2006). Consumer adoption of net-enabled intermediaries: Theoretical explanation and an empirical test. *Journal of the Association for Information Systems*, 7(7), 473–508.

Spiekermann, S., & Novotny, A. (2015). A vision for global privacy bridges: Technical and legal measures for international data markets. *Computer Law & Security Review*, 31(2), 181–200. doi:10.1016/j.clsr.2015.01.009

Stokes, J., Childs, L., & Fuehrer, A. (1981). Gender and sex roles as predictors of self-disclosure. *Journal of Counseling Psychology*, 28(6), 510–514. doi:10.1037/0022-0167.28.6.510

Taylor, D. G., Davis, D. F., & Jillapalli, R. (2009). Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research*, 9(3), 203–223. doi:10.1007/s10660-009-9036-2

Wakefield, R. (2013). The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems*, 22(2), 157–174. doi:10.1016/j.jsis.2013.01.003

Wang, E. T., Yeh, H.-Y., & Jiang, J. J. (2006). The relative weights of internet shopping fundamental objectives: Effect of lifestyle differences. *Psychology and Marketing*, 23(5), 353–367. doi:10.1002/mar.20116

Weible, R. J. (1993). *Privacy and Data: An Empirical Study of the Influence of Types of Data and Situational Context Upon Privacy Perceptions*. Mississippi State University. Department of Business and Industry.

Westin, A. F. (1966). Science, privacy, and freedom: Issues and proposals for the 1970's. Part I--The current impact of surveillance on privacy. *Columbia Law Review*, 66(6), 1003. doi:10.2307/1120997

Westin, A. F. (1991). Harris-Equifax Consumer Privacy Survey. Atlanta, GA.

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. doi:10.1007/s11002-006-4147-1

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

Yang, S., & Wang, K. (2009). The influence of information sensitivity compensation on privacy concern and behavioral intention. *The DATA BASE for Advances in Information Systems*, 40(1), 38–51.

Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology*, 58(5), 710–722. doi:10.1002/asi.20530

7. Appendices

Appendix A Results of pre-test

Table A.1 Results of the pre-test regarding frequency of requested items

	Frequency	Mean (SD)
Name	25	4.76 (0.83)
Address	25	4.76 (0.83)
Email address	25	4.72 (0.84)
Phone number	25	4.08 (0.86)
Bank information	24	3.67 (1.52)
Birthdate and -place	25	3.52 (1.36)
Credit card number	24	3.25 (1.45)
Gender	25	2.92 (1.32)
Age	25	2.88 (1.13)
Occupation	25	1.80 (0.91)
Number of people in household	25	1.52 (0.77)
Hobbies and interests	25	1.52 (0.96)
Recent purchases online	25	1.52 (0.87)
Product preferences	25	1.48 (0.82)
Education	25	1.36 (0.76)
Type of Internet access	25	1.32 (0.75)
Time spent online (last 7 days)	25	1.32 (0.80)
Marital status	25	1.28 (0.61)
Internet devices	25	1.24 (0.52)
Favorite TV-Channel	25	1.20 (0.50)
Watched TV-Programs (last 7 days)	25	1.20 (0.50)
Read magazines (last 30 days)	25	1.20 (0.50)
Read newspapers (last 7 days)	25	1.20 (0.50)
Height	25	1.20 (0.65)
Monthly income	24	1.17 (0.56)
Ownership or rental of home	25	1.16 (0.47)
Weight	25	1.08 (0.28)
Organ donor	24	1.04 (0.20)
Social Security Number	25	1.04 (0.20)
Sexual orientation	25	1.04 (0.20)
Political party affiliation	25	1.04 (0.20)
Amount of cars owned	25	1.00 (0.00)
Ethnic group	25	1.00 (0.00)
Name of health insurance company	24	1.00 (0.00)
Blood type	25	0.92 (0.40)

Notes. Measured on a 5-point Likert-scale (1 = very unlikely, 5 = very likely). The items included in the actual study are indicated in bold. The item Age was deleted because it was similar to Birthdate and -place. The item credit card number was deleted because it was similar to bank information.

Appendix B Original survey in German

Willkommen zu dem Abschlussprojekt meines Masterprogrammes, danke schön, dass Sie sich bereit erklären an meiner Umfrage über die Weitergabe von persönlichen Informationen an Online-Shops teilzunehmen. In dem ersten Teil werden Sie einen kurzen Text über ein Unternehmen lesen und deren Webseite sehen. Anschließend bitte ich Sie das Unternehmen und dessen Anfrage zu beurteilen. Bitte lesen Sie den Text sorgfältig durch und bedenken Sie, dass sie im Anschluss Fragen zu dem präsentierten Unternehmen beantworten werden. Es werden lediglich Ihre Meinung und Einstellung abgefragt, nicht Ihr Wissen - es gibt keine richtigen oder falschen Antworten. Die Umfrage sollte nicht mehr als 10 Minuten Ihrer Zeit in Anspruch nehmen. Versuchen Sie bitte die Umfrage in einem Durchgang zu beenden. Die Ergebnisse werden nicht auf Sie als individuelle/ individueller TeilnehmerIn zurückzuführen sein. Mit freundlichen Grüßen, Sabrina Kaul Masterstudentin (Communication Studies) an der University of Twente

☐ Ich erkläre mich freiwillig bereit an dieser Forschung teilzunehmen

MGS

Stellen Sie sich vor, dass Sie ein Buch kaufen möchten. Amazon.de hat dieses die nächsten paar Monate nicht auf Lager und nur eine geringe Anzahl an Webseiten bietet es momentan an. Weil Sie das Buch sehr dringend benötigen, gehen Sie auf Weltderbücher.de. Die bekannte Shopping-Seite für Bücher und E-books bietet es zum gleichen Preis an, wie die anderen Anbieter. Erst letzte Woche haben Sie etwas über die Webseite in einem Artikel in der Zeit gelesen. In dem Artikel steht, dass Weltderbücher.de den Preis für „Bester Kundenservice“ von Stiftung Warentest verliehen bekommen hat. Darüber hinaus erklärt der Artikel, dass Weltderbücher.de verlässlich beim Versenden seiner Ware ist und klare Umtausch- und Rücksenderichtlinien hat. Obwohl Sie noch nie etwas bei weltderbücher.de bestellt haben, entscheiden Sie sich dafür das Buch hier zu kaufen. Bevor Sie jedoch die Kasse erreichen, werden Sie gebeten an einer Umfrage von Weltderbücher.de teilzunehmen (siehe unten). Sie brauchen den Fragebogen nicht auszufüllen, um mit Ihrer Bestellung fortzufahren, aber Sie würden einen Gutschein über 25 Euro auf Ihre nächste Bestellung erhalten, wenn Sie sich doch dazu entscheiden sollten.

MGP

Stellen Sie sich vor, dass Sie ein Buch kaufen möchten. Amazon.de hat dieses die nächsten paar Monate nicht auf Lager und nur eine geringe Anzahl an Webseiten bietet es momentan an. Weil Sie das Buch sehr dringend benötigen, gehen Sie auf Weltderbücher.de. Die bekannte Shopping-Seite für Bücher und E-books bietet es zum gleichen Preis an, wie die anderen Anbieter. Erst letzte Woche haben Sie etwas über die Webseite in einem Artikel in der Zeit gelesen. In dem Artikel steht, dass Weltderbücher.de den Preis für „Beste Datenschutzerklärung“ von Stiftung Warentest verliehen bekommen hat. Darüber hinaus erklärt der Artikel, dass Weltderbücher.de den nationalen Regulierungen zum Schutz der Privatsphäre von Kunden nachkommt. Obwohl Sie noch nie etwas bei weltderbücher.de bestellt haben, entscheiden Sie sich dafür das Buch hier zu kaufen. Bevor Sie jedoch die Kasse erreichen, werden Sie gebeten an einer Umfrage von Weltderbücher.de teilzunehmen (siehe unten). Sie brauchen den Fragebogen nicht auszufüllen, um mit Ihrer Bestellung fortzufahren, aber Sie würden einen Gutschein über 25 Euro auf Ihre nächste Bestellung erhalten, wenn Sie sich doch dazu entscheiden sollten.

MB

Stellen Sie sich vor, dass Sie ein Buch kaufen möchten. Amazon.de hat dieses die nächsten paar Monate nicht auf Lager und nur eine geringe Anzahl an Webseiten bietet es momentan an. Weil Sie das Buch sehr dringend benötigen, gehen Sie auf Weltderbücher.de. Die bekannte Shopping-Seite für Bücher und E-books bietet es

zum gleichen Preis an, wie die anderen Anbieter. Erst letzte Woche haben Sie etwas über die Webseite in einem Artikel in der Zeit gelesen. In dem Artikel stand, dass Weltderbücher.de bei einem Test von Stiftung Warentest in den Kategorien Kunden- und Versandservice sehr schlecht abgeschnitten habe. Darüber hinaus soll Weltderbücher.de eine unbefriedigende Datenschutzerklärung haben, die die nationalen Regulierungen zum Schutz der Privatsphäre der Kunden nicht erfüllt. Obwohl Sie noch nie etwas bei weltderbücher.de bestellt haben, entscheiden Sie sich dafür das Buch hier zu kaufen. Bevor Sie jedoch die Kasse erreichen, werden Sie gebeten an einer Umfrage von Weltderbücher.de teilzunehmen (siehe unten). Sie brauchen den Fragebogen nicht auszufüllen, um mit Ihrer Bestellung fortzufahren, aber Sie würden einen Gutschein über 25 Euro auf Ihre nächste Bestellung erhalten, wenn Sie sich doch dazu entscheiden sollten.

NGS

Stellen Sie sich vor, dass Sie ein Buch kaufen möchten. Amazon.de hat dieses die nächsten paar Monate nicht auf Lager und nur eine geringe Anzahl an Webseiten bietet es momentan an. Weil Sie das Buch sehr dringend benötigen, gehen Sie auf Weltderbücher.de. Die bekannte Shopping-Seite für Bücher und E-books bietet es zum gleichen Preis an, wie die anderen Anbieter. Erst letzte Woche haben Sie etwas über die Webseite in einem Artikel in der Zeit gelesen. In dem Artikel steht, dass Weltderbücher.de den Preis für „Bester Kundenservice“ von Stiftung Warentest verliehen bekommen hat. Darüber hinaus erklärt der Artikel, dass Weltderbücher.de verlässlich beim Versenden seiner Ware ist und klare Umtausch- und Rücksenderichtlinien hat. Obwohl Sie noch nie etwas bei weltderbücher.de bestellt haben, entscheiden Sie sich dafür das Buch hier zu kaufen. Bevor Sie jedoch die Kasse erreichen, werden Sie gebeten an einer Umfrage von Weltderbücher.de teilzunehmen (siehe unten). Sie brauchen den Fragebogen nicht auszufüllen, um mit Ihrem Kauf fortzufahren. Sie würden jedoch Zugriff auf drei Kapitel aus dem Buch Ihrer Wahl noch bevor dem offiziellen Erscheinungsdatum erhalten, wenn Sie sich doch dazu entscheiden sollten. Außerdem bekommen Sie eine signierte Ausgabe des Buches, falls Sie sich zum Kauf entschließen.

NGP

Stellen Sie sich vor, dass Sie ein Buch kaufen möchten. Amazon.de hat dieses gerade nicht auf Lager und nur eine geringe Anzahl an Webseiten bietet es momentan an. Weltderbücher.de bietet es zum gleichen Preis an, wie die anderen Anbieter. Es ist eine bekannte Shopping-Seite für Bücher und E-books. Erst letzte Woche haben Sie etwas über die Webseite in einem Artikel in der Zeit gelesen. In dem Artikel steht, dass Weltderbücher.de die Preise für „Bester Kundenservice“ und „Höchste Sicherheitsstandards“ von Stiftung Warentest verliehen bekommen hat. Der Artikel verweist auch auf eine Studie unter jungen Deutschen, die besagt, dass Weltderbücher.de verlässlich und vertrauenswürdig ist. Darüber hinaus erklärt der Artikel, dass Weltderbücher.de den nationalen Regulierungen zum Schutz der Privatsphäre von Kunden nachkommt. Obwohl Sie noch nie etwas bei weltderbücher.de bestellt haben, entscheiden Sie sich dafür das Buch hier zu kaufen. Bevor Sie jedoch die Kasse erreichen, werden Sie gebeten an einer Umfrage von Weltderbücher.de teilzunehmen (siehe unten). Sie brauchen den Fragebogen nicht auszufüllen, um mit Ihrem Kauf fortzufahren. Sie würden jedoch Zugriff auf drei Kapitel aus dem Buch Ihrer Wahl noch bevor dem offiziellen Erscheinungsdatum erhalten, wenn Sie sich doch dazu entscheiden sollten. Außerdem bekommen Sie eine signierte Ausgabe des Buches, falls Sie sich zum Kauf entschließen.

NB

Stellen Sie sich vor, dass Sie ein Buch kaufen möchten. Amazon.de hat dieses die nächsten paar Monate nicht auf Lager und nur eine geringe Anzahl an Webseiten bietet es momentan an. Weil Sie das Buch sehr dringend benötigen, gehen Sie auf Weltderbücher.de. Die bekannte Shopping-Seite für Bücher und E-books bietet es zum gleichen Preis an, wie die anderen Anbieter. Erst letzte Woche haben Sie etwas über die Webseite in einem Artikel in der Zeit gelesen. In dem Artikel stand, dass Weltderbücher.de bei einem Test von Stiftung Warentest in den Kategorien Kunden- und Versandservice sehr schlecht abgeschnitten habe. Darüber hinaus

soll Weltderbücher.de eine unbefriedigende Datenschutzerklärung haben, die die nationalen Regulierungen zum Schutz der Privatsphäre der Kunden nicht erfüllt. Obwohl Sie noch nie etwas bei weltderbücher.de bestellt haben, entscheiden Sie sich dafür das Buch hier zu kaufen. Bevor Sie jedoch die Kasse erreichen, werden Sie gebeten an einer Umfrage von Weltderbücher.de teilzunehmen (siehe unten). Sie brauchen den Fragebogen nicht auszufüllen, um mit Ihrem Kauf fortzufahren. Sie würden jedoch Zugriff auf drei Kapitel aus dem Buch Ihrer Wahl noch bevor dem offiziellen Erscheinungsdatum erhalten, wenn Sie sich doch dazu entscheiden sollten. Außerdem bekommen Sie eine signierte Ausgabe des Buches, falls Sie sich zum Kauf entschließen.

Bitte geben Sie auf einer Skala von 1 (sehr schlechter Ruf) bis 5 (sehr guter Ruf) an, wie Sie das gezeigte Unternehmen einstufen würden.

- ☐ Sehr schlechter Ruf (1)
- ☐ Schlechter Ruf (2)
- ☐ Weder schlechter noch guter Ruf (3)
- ☐ Guter Ruf (4)
- ☐ Sehr guter Ruf (5)

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

	Trifft nicht zu (1)	Trifft eher nicht zu (2)	Teils-teils (3)	Trifft eher zu (4)	Trifft zu (5)
Weltderbücher.de hat einen guten Kundenservice (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Weltderbücher.de hat gute Versand- und Rücksenderichtlinien (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Weltderbücher.de kommt den nationalen Regulierungen zum Privatsphärenschutz nach (3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Weltderbücher.de hat eine gute Datenschutzerklärung (4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Bitte geben Sie an, wie sehr Sie auf einer Skala von 1 (trifft nicht zu) bis 5 (trifft zu) mit den folgenden Aussagen über die Möglichkeit einer zu erhaltenden Belohnung auf der Basis des gesehenen Szenarios übereinstimmen.

	Trifft nicht zu (1)	Trifft eher nicht zu (2)	Teils-teils (3)	Trifft eher zu (4)	Trifft zu (5)
Ich erhalte einen 25€ Gutschein, wenn ich den präsentierten Fragebogen ausfülle (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich erhalte Zugang zu drei Kapiteln aus dem Buch meiner Wahl vor Veröffentlichung, wenn ich den präsentierten Fragebogen ausfülle (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Bitte geben Sie auf einer Skala von 1 (viel niedriger) bis 5 (viel höher) an, wie Sie den Wert der angebotenen Belohnung im Vergleich zum Wert Ihrer persönlichen Informationen einschätzen.

- ☐ Viel niedriger (1)
- ☐ Niedriger (2)
- ☐ Ungefähr gleich (3)
- ☐ Höher (4)
- ☐ Viel höher (5)

Bitte geben Sie auf einer Skala von 1 (trifft nicht zu) bis 5 (trifft zu) an, wie sehr Sie mit den Aussagen über die angebotenen Belohnung übereinstimmen.

	Trifft nicht zu (1)	Trifft eher nicht zu (2)	Teils-teils (3)	Trifft eher zu (4)	Trifft zu (5)
Die vom Unternehmen angebotene Belohnung ist attraktiv für mich (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Die vom Unternehmen angebotene Belohnung ist angemessen (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Die vom Unternehmen angebotene Belohnung ist wertvoll (3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Die vom Unternehmen angebotene Belohnung ist nützlich (4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Die vom Unternehmen angebotene Belohnung verschafft mir einen Vorteil (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Bitte geben Sie auf einer Skala von 1 (Sehr unwahrscheinlich) bis 5 (Sehr wahrscheinlich) an, wie wahrscheinlich es ist, dass Sie die gefragten Informationen an das präsentierte Unternehmen preisgegeben hätten.

	Sehr unwahr- scheinlich (1)	Unwahr- scheinlich (2)	Unentschieden (3)	Wahr- scheinlich (4)	Sehr wahrscheinlich (5)
Name (37)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Adresse (38)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sozialversicherungs- nummer (39)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Email-Adresse (40)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Telefonnummer (41)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Bankinformationen (42)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Anzahl Personen im Haushalt (43)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Miete oder Eigentum (44)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Anzahl Autos (45)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kürzliche Einkäufe online (46)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Art des Internetzugangs (47)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Hobbys und Interessen (48)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Beruf (49)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vorliebe für bestimmte Produkte (50)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Stunden verbracht online (in den letzten 7 Tagen) (51)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sexuelle Orientierung (52)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Politische Zugehörigkeit (53)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Bildung (54)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Blutgruppe (55)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Name der Krankenversicherung (56)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Organspender (57)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Gewicht (58)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Geburtsdatum- und Ort (59)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Geschlecht (60)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ethnische Zugehörigkeit (61)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Bitte geben Sie auf einer Skala von 1 (überhaupt nicht beunruhigt) bis 5 (sehr beunruhigt) an, wie besorgt Sie sind, wenn Sie die folgenden Informationen preisgeben.

	Überhaupt nicht beunruhigt (1)	Weniger beunruhigt (2)	Unentschieden (3)	Beunruhigt (4)	Sehr beunruhigt (5)
Name (37)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Adresse (38)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sozialversicherungsnummer (39)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Email-Adresse (40)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Telefonnummer (41)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Bankinformationen (42)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Anzahl Personen im Haushalt (43)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Miete oder Eigentum (44)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Anzahl Autos (45)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kürzliche Einkäufe online (46)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Art des Internetzugangs (47)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Hobbys und Interessen (48)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Beruf (49)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vorliebe für bestimmte Produkte (50)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Stunden verbracht online (in den letzten 7 Tagen) (51)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sexuelle Orientierung (52)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Politische Zugehörigkeit (53)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Bildung (54)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Blutgruppe (55)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Name der Krankenversicherung (56)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Organspender (57)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Gewicht (58)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Geburtsdatum- und Ort (59)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Geschlecht (60)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ethnische Zugehörigkeit (61)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Bitte geben Sie auf einer Skala von 1 (Trifft nicht zu) bis 5 (Trifft zu) an, wie sehr Sie mit den Aussagen über die Sorgen um den Schutz der Privatsphäre im Zusammenhang mit der präsentierten Unternehmenswebseite übereinstimmen.

	Trifft nicht zu (1)	Trifft eher nicht zu (2)	Teils-teils (3)	Trifft eher zu (4)	Trifft zu (5)
Ich bin beunruhigt, dass die Webseite zu viele Informationen über mich sammelt. (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Es stört mich, wenn die Webseite mich nach persönlichen Informationen fragt. (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich habe Sorge um meine Privatsphäre, wenn ich auf dieser Webseite stöbere. (3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich habe Zweifel daran, dass meine Privatsphäre auf dieser Webseite gut genug geschützt ist. (4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Meine persönlichen Informationen könnten missbraucht werden, wenn ich ein Geschäft über diese Webseite abwickele. (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Unbekannte Dritten könnten sich Zugang zu meinen persönlichen Informationen verschaffen, wenn ich ein Geschäft über diese Webseite abwickele. (6)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Bitte geben Sie auf einer Skala von 1 (Trifft nicht zu) bis 5 (Trifft zu) an, wie sehr Sie mit den Aussagen über allgemeine Einstellungen zu Privatsphäre übereinstimmen.

	Trifft nicht zu (1)	Trifft eher nicht zu (2)	Teils-teils (3)	Trifft eher zu (4)	Trifft zu (5)
Verglichen mit anderen bin ich empfindlicher, wenn es darum geht wie Unternehmen meine persönlichen Informationen verarbeiten. (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Für mich ist es das Wichtigste, dass meine Informationen privat bleiben. (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Verglichen mit anderen bin ich eher um die Gefahren besorgt, die meine Privatsphäre bedrohen. (3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich ziehe es vor, dass andere wenig über mich wissen. (4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Im Allgemeinen brauche ich viel Platz um mich herum. (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Es gibt viele Dinge, über die ich nicht mit anderen rede. (6)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich finde es wichtig, dass ich die Kontrolle darüber habe, wer meine persönlichen Informationen benutzen kann. (7)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich finde es wichtig, dass ich die Kontrolle darüber habe, wer Zugang zu meinen persönlichen Informationen erhält. (8)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich bin davon überzeugt, dass meine Privatsphäre respektiert und geschützt werden sollte. (9)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Was ist Ihr Geschlecht?

- ☐ Männlich (1)
- ☐ Weiblich (2)

Wie alt sind Sie?

Welchen höchsten Bildungsabschluss haben Sie?

- ☐ Keinen Abschluss (1)
- ☐ Mittlerer Schulabschluss (2)
- ☐ Berufsausbildung (3)
- ☐ (Fach-) Abitur (7)
- ☐ Bachelorabschluss oder vergleichbar (4)
- ☐ Masterabschluss oder vergleichbar (5)
- ☐ Dokortitel (6)
- ☐ Anderer (8) _____

Wie hoch ist Ihr monatliches Einkommen? (Falls Sie kein geregeltes Einkommen haben - wie viel Geld steht Ihnen in der Regel im Monat zur freien Verfügung?)

- ☐ weniger als € 1.400 (1)
- ☐ € 1.400 - € 2.500 (2)
- ☐ € 2.501 - € 4.000 (3)
- ☐ € 4.001 - € 10.000 (4)
- ☐ mehr als € 10.000 (5)

Seit wie vielen Jahren benutzen Sie das Internet?

Wie oft kaufen Sie Produkte online?

- ☐ Nie (1)
- ☐ Weniger als einmal im Monat (2)
- ☐ Einmal im Monat (3)
- ☐ 2 bis 3 Mal im Monat (4)
- ☐ Einmal die Woche (5)
- ☐ 2 bis 3 Mal die Woche (6)
- ☐ Täglich (7)

Appendix C Factor analyses

Table C.1 First factorial analysis of willingness to disclose personal information

Items	Components		
	1	2	3
Number of people in household	.818		
Recent purchases online	.789		
Amount of cars owned	.783		
Hobbies and interests	.772		
Type of Internet access	.763		
Time spent online (last 7 days)	.760		
Ownership or rental of home	.748		
Occupation	.745		
Education	.724		
Product preferences	.701		
Ethnic group	.585		
Political party affiliation		.801	
Sexual orientation		.780	
Blood type		.704	
Name of health insurance company		.701	
Organ donor		.669	
Weight		.647	
Name			.888
Address			.874
Email address			.868
Phone number			.563
Gender			.553
Bank information			.544
Birthdate and -place			
Social security number			.718

Notes. Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.

Table C.2 First factorial analysis of level of concern about disclosing information

Items	Components			
	1	2	3	4
Amount of cars owned	.834			
Recent purchases online	.826			
Type of Internet access	.808			
Hobbies and interests	.807			
Number of people in household	.797			
Time spent online (last 7 days)	.765			
Product preferences	.757			
Ownership or rental of home	.756			
Occupation	.748			
Education	.653			
Political party affiliation		.811		
Organ donor		.784		
Name of health insurance company		.782		
Blood type		.781		
Sexual orientation		.757		
Weight		.683		
Ethnic group		.634		
Name			.840	
Address			.804	
Email address			.755	
Phone number			.623	
Gender			.577	
Birthdate and -place			.533	
Social security number				.745
Bank information				.545

Notes. Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.

Table C.3 Final factorial analysis of level of concern about disclosing information

Items	Components		
	1	2	3
Hobbies and interests	.841		
Recent purchases online	.833		
Amount of cars owned	.821		
Type of Internet access	.818		
Number of people in household	.804		
Product preferences	.788		
Time spent online (last 7 days)	.784		
Occupation	.771		
Ownership or rental of home	.728		
Education	.679		
Political party affiliation		.813	
Name of health insurance company		.803	
Organ donor		.797	
Sexual orientation		.755	
Weight		.655	
Address			.868
Name			.834
Phone number			.714
Email address			.701
Bank information			.588

Notes. Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.

Table C.4 Items and reliability of the constructs used in the study

Scales and items	Components		
	1	2	3
<i>Value of incentive</i>			
• The worth of the compensation offered by the company in comparison to the worth of the requested information about yourself ^a	.562		
• The compensation offered by the company for my information is attractive ^b	.871		
• The compensation offered by the company for my information is appropriate ^b	.780		
• The compensation offered by the company for my information is valuable ^b	.850		
• The compensation offered by the company for my information is beneficial ^b	.776		
• The compensation offered by the company for my information is advantageous ^b	.760		
<i>Personal privacy evaluation</i>			
• Compared to others, I am more sensitive about the way companies handle my personal information ^b			.889
• To me, it is the most important thing to keep my information private ^b			.856
• Compared to others, I tend to be more concerned about threats to my privacy ^b			.921
<i>Privacy concerns</i>			
• I am concerned that the website is collecting too much information about me ^b		.773	
• It bothers me when the website asks me for personal information ^b		.759	
• I am concerned about my privacy when browsing this website ^b		.798	
• I have doubts as to how well my privacy is protected on this website ^b		.873	
• My personal information could be misused when transacting with this website ^b		.869	
• My personal information could be accessed by unknown parties when transacting with this website ^b		.803	

Notes. Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization. ^a Measured on a 5-point Likert-scale (1 = much lower, 5 = much higher). ^b Measured on a 5-point Likert-scale (1 = strongly disagree, 5 = strongly agree).

Appendix D Post-hoc analysis for MANCOVA

Table D.1 Post-hoc analysis with Bonferroni pairwise comparison of the dependent variables among corporate reputation conditions

	<i>p</i>					
	PS		PP		N	
	PP	N	PS	N	PS	PP
Identification	1	0,145	1	0,357	0,145	0,357
Lifestyle	1	0,134	1	0,47	0,134	0,47
Sensitive Information	1	1	1	1	1	1
Privacy Concerns	1	0,017	1	<.001	0,017	<.001

Notes. PS = Positive corporate reputation - Service performance, PP = Positive corporate reputation - Privacy protection, N = Negative corporate reputation

Appendix E Regression analysis

Table E.1 Coefficients of the dependent variables influenced by personal privacy evaluation, and value of incentive

	<i>B</i>	Std. error	β	<i>t</i>	<i>p</i>	<i>F</i>	<i>R</i> ²	Adj. <i>R</i> ²
<i>Identification</i>								
• Constant	3.23	0.23		14.06	.000	21.08	.10	.10
• Personal Privacy Evaluation	-0.24	0.05	-.25***	-4.90	.000			
• Value of Incentive	0.16	0.05	.17***	3.41	.001			
<i>Lifestyle</i>								
• Constant	2.05	0.22		9.21	.000	37.65	.17	.17
• Personal Privacy Evaluation	-0.21	0.05	-.21***	-4.41	.000			
• Value of Incentive	0.30	0.04	.32***	6.66	.000			
<i>Sensitive Information</i>								
• Constant	1.38	1.54		8.92	.000	9.95	.05	.05
• Personal Privacy Evaluation	-0.09	0.03	-.13***	-2.54	.011			
• Value of Incentive	0.10	0.03	.17***	3.21	.001			
<i>Privacy Concerns</i>								
• Constant	3.69	0.18		20.65	.000	60.97	.25	.25
• Personal Privacy Evaluation	0.30	0.04	.36***	7.87	.000			
• Value of Incentive	-0.22	0.04	-.29***	-6.37	.000			

Note. ****p* < .001

Table E.2 Coefficients of the dependent variables influenced by privacy concerns

	<i>B</i>	Std. error	β	<i>t</i>	<i>p</i>	<i>F</i>	R^2	Adj. R^2
<i>Identification</i>								
• Constant	3.67	.26		13.93	.000			
• Privacy Concerns	-.22	.06	-.19***	-3.61	.000	13.07	.03	.03
<i>Lifestyle</i>								
• Constant	3.56	.26		13.90	.000			
• Privacy Concerns	-.37	.06	-.31***	-6.21	.000	38.56	.10	.09
<i>Sensitive Information</i>								
• Constant	2.09	.17		12.27	.000			
• Privacy Concerns	-.18	.04	-.24***	-4.65	.000	21.37	.06	.05

Note. *** $p < .001$