WHY ARE CONSUMERS WILLING TO PAY FOR PRIVACY? AN APPLICATION OF THE PRIVACY-FREEMIUM MODEL TO MEDIA COMPANIES

Complete Research

Schreiner, Michel, Ludwig-Maximilians-Universität München, Munich, Germany, schreiner@bwl.lmu.de

Hess, Thomas, Ludwig-Maximilians-Universität München, Munich, Germany, thess@bwl.lmu.de

Abstract

Monetizing their users' personal information instead of charging a fee has become an established revenue model for platform operators—a new form of media companies specialized in aggregating, managing, and distributing user-generated online content. However, the commodification of privacy leads to privacy concerns that might be a risk for such businesses. Thus, a new approach is to focus on consumers' willingness to pay for privacy, assuming that monetizing privacy protection might be an alternative revenue model. Following the freemium idea, we developed an innovative research design, offering 553 online survey participants the opportunity to subscribe to a fictional premium version of Facebook with additional privacy control features in return for a monthly fee. Based on the theory of planned behavior, we developed and tested a research model to explain actual willingness to pay for privacy behavior. Our findings show that perceived usefulness and trust significantly affect willingness to pay. In contrast, perceived internet privacy risk was not found to have a significant influence. We thus conclude that consumers are willing to pay for privacy in the form of a privacy-freemium model, provided they perceive the premium version as offering added value and as trustworthy.

Keywords: Privacy-Freemium Model, Willingness to Pay, Media Companies, Facebook.

1 Introduction

The traditional view of media companies is based on the idea of publishing or broadcasting content that is typically produced or aggregated by professionals. This understanding, however, no longer seems adequate in the internet age. Since users have been enabled to produce their own content, Hess (2014) suggests that a new form of media companies—the *platform operators* who aggregate, manage, and distribute user-generated content—has emerged. He therefore distinguishes between two types of media companies: First, content providers creating, bundling, and distributing content follow the publishing-broadcasting approach (e.g. newspaper publishers, broadcasting stations, etc.). This approach also includes first generation online offerings based on the same value chain (e.g. online offers of newspapers and broadcasting stations, etc.). Second, media companies following the platform approach run an IT-based platform to attract and distribute content that is provided by users. This type of media companies comprises second generation online offerings, such as market places, search engines, and social networks. While the publishing-broadcasting approach corresponds to the traditional understanding of a media company as a content provider, running an IT-based platform primarily characterizes content platform operators, who therefore specifically address the intersection between media management and information systems.

However, content providers and platform operators have, so far, generally struggled to find viable and stable revenue models when offering online content (see Lopes and Galletta, 2006). Traditionally, media companies generate revenues either indirectly by selling the obtained attention for advertising purposes, or directly through paid content (Hess, 2014). One way to attract the attention of a wide audience, and thus achieve high advertisement revenues, is offering online content for free. Although advertisement revenues have become an established revenue model for media companies on the internet, they are sensitive to fluctuations in the economic climate (Chyi, 2012). Furthermore, providing content for free runs the risk of cannibalizing the own offline offerings and paid-content revenues—a problem that especially concerns content providers (see, e.g. the current newspaper crisis). In addition, it has been shown that consumers' willingness to pay (WTP) for online content is generally weak (Chyi, 2012). Hence, *freemium* has currently gained popularity as a new revenue model for media companies. The concept is based on the idea of providing offerings free of charge, generally with the opportunity to earn advertisement revenues (Anderson, 2009), while at the same time providing fee-based offerings that allow access to premium content or features, and thus enhancing consumers' WTP (Wagner et al., 2014). Although freemium seems to have become an established approach, especially for content providers, platform operators have so far specialized in another revenue model.

Owing to its character as an interactive medium, the internet facilitates gathering an increasing amount of personal information on users and their behaviors, while providing the technological infrastructure to collect, store, analyze, and distribute it. Platform operators have already recognized the great potential of the resulting commercial opportunities and have established new business and revenue models to profit from their users' personal information. For instance, platform operators use personal information to personalize their services in order to enhance the user experience and future convenience (see Hann et al., 2007; Kobsa, 2007). Furthermore, personal information is used to increase the efficiency and profitability of advertising and marketing efforts by optimizing targeting procedures, enhancing cross-selling potentials through smarter recommender systems, and even achieving maximum profits based on price discrimination (see Acquisti and Varian, 2005; Toch et al., 2012). Finally, since personal information is likewise also very valuable for other companies, platform operators provide, rent, or sell it to their affiliates, business partners, and third parties (Gomez et al., 2009). Consequently, monetizing personal information instead of charging a fee for using a content platform has become a very successful revenue model on the internet.

However, the commodification of privacy is one of the strongest contributors to arising information privacy concerns that, at least in the long run, might be a business risk for operators if users consequently restrict their platform use or terminate it (Krasnova et al., 2010). Hence, a new approach is to focus on consumers' WTP for privacy. This approach is based on the assumption that, while some consumers prefer using a given content platform free of charge in exchange for providing personal information, others might prefer paying to protect their privacy. While previous studies have dealt with the WTP for privacy, very few have looked into WTP with regard to content platforms. For instance, Krasnova et al. (2009) conducted a conjoint analysis to investigate the value of privacy in online social networks. They found that users differ with regard to their need for privacy. Hence, the authors suggest that network providers might monetize their members' different privacy preferences in the form of various premium accounts. Schreiner et al. (2013) followed this approach and found the optimal pricing point for a premium version of Facebook containing additional privacy-enhancing functionalities to be 1.67 euro per month. Taking this into account, a *privacy-freemium model* might be the answer to both questions—how to earn money from user-generated online content and, simultaneously, how to solve consumers' privacy concerns when using a content platform.

However, while previous studies have shown evidence of the pricing of a privacy-freemium model for social networks, they lack a theoretically based explanation of *why consumers are willing to pay for privacy*. Furthermore, regarding the applied hypothetical research designs, rather more WTP for privacy intentions than de facto behaviors have been observed in prior work. Thus, we aim to close this gap by applying the theory of planned behavior (TPB) (Ajzen, 1991) in order to explain actual WTP for privacy behavior, using the example of a fictional premium version of Facebook. Specifically, based

on an online survey, we examine the determinants affecting Facebook users' WTP for privacy intention and their de facto behavior when offering them the opportunity to subscribe to a premium version of the platform, which provides additional privacy control features in return for a monthly fee.

The paper is structured as follows: The next section describes the study's theoretical background by discussing related work on the WTP for privacy and explaining the research model and hypotheses development. Thereafter, we describe the research design and data collection. The data analysis and results are presented in Section 4. An overall summary of the study and a discussion of its implications and limitations conclude the paper.

2 Theoretical Background

2.1 Related work

A large body of the information privacy literature refers to a control-based definition of privacy that originates from Westin's (1967) and Altman's (1975) theories of general privacy (Smith et al., 2011). We follow this strand of literature and understand privacy as "the ability of individuals to control the terms under which their personal information is acquired and used" (Culnan and Bies, 2003, p. 326). Furthermore, the privacy calculus is a well-established concept to explain individuals' privacy-related behaviors. In the context of our research focus, this concept addresses the impact of privacy concerns on consumers' decision making and behavior, assuming that users of a content platform consider the consequences of their actions in the form of a trade-off between costs and benefits (see Dinev and Hart, 2006; Smith et al., 2011). This calculus view of information privacy suggests that users are able to perform a rational risk-benefit analysis to assess what they would gain in exchange for providing personal information, like financial rewards, as well as personalization and social adjustment benefits (Smith et al., 2011). Further, this view suggests that they would trade their privacy provided the achievable benefits outweigh, or at least compensate for, the risks involved (Chellappa and Sin, 2005; Culnan and Bies, 2003). However, although the privacy calculus was originally developed to describe personal information disclosure, it can be adapted to the WTP for privacy context, assuming that users might be willing to pay for privacy, or, more precisely, for reducing their privacy risk.

Previous research has shown conflicting evidence of consumers' WTP for privacy. For instance, in an experimental study on purchasing behavior, Tsai et al. (2011) indicate that consumers are willing to pay a price premium in order to buy from online retailers who protect their privacy better, if privacy policy information is made more salient and accessible. The authors thus conclude "that businesses may be able to leverage privacy protection as a selling point." Using the example of e-books, audiobooks, and textbooks, Mai et al. (2010) find that online vendors bearing privacy seals charge a price premium of 1.5 percent compared to vendors without such a seal. This result also indicates consumers' WTP for privacy. Additionally, in a recent study, Egelman et al. (2013) show "that many smartphone users are concerned with their privacy and are willing to pay premiums for applications that are less likely to request access to personal information […]."

In contrast, other work has found no or only limited WTP for privacy. For instance, Grossklags and Acquisti (2007) demonstrate that willingness to accept a proposal to sell personal information is much higher than the WTP for protecting it. In another experimental study, Beresford et al. (2010) find that consumers are unwilling to pay for privacy in the context of e-commerce transactions, even though almost all the participants indicated that they are interested in the protection of their personal information. This phenomenon has generally been denoted as the privacy paradox, since consumers' privacy actions do not necessarily correspond to their attitudes and/or their behavioral intentions (Norberg et al., 2007). Taking the privacy paradox into consideration, Acquisti (2004), as well as Acquisti and Grossklags (2005), suggest that even individuals who may genuinely want to protect their privacy might not do so because their privacy-related decision making is affected by bounded rationality. In particular, by taking the behavioral economics literature's assumptions about hyperbolic discounting

and immediate gratification into account, they argued that individuals generally tend to discount future costs or benefits, and are therefore likely to trade off their long-term privacy for short-term benefits (e.g. providing personal information in exchange for a content platform's immediate gratis use).

However, since we focus on an application of the privacy-freemium model to media companies, this study examines consumers' WTP for privacy in a special context. Thus, while prior work has provided an explanation of privacy actions referring to behavioral economics, we provide a different perspective by applying the TPB in order to examine the determinants affecting consumers' WTP for privacy when privacy protection is offered in the form of a premium version of Facebook. Nevertheless, taking the privacy paradox into consideration, we not only observe WTP for privacy intentions in this study, but also actual WTP for privacy behaviors.

2.2 Research model and hypotheses development

Several established theories in the information systems discipline can be applied to explain consumers' intention to use the fee-based premium version of Facebook or their use behavior. For instance, the technology acceptance model (TAM) (Davis et al., 1989), the unified theory of acceptance and use of technology (UTAUT) (Venkatesh et al., 2003), as well as its most recent form UTAUT2 (Venkatesh et al., 2012), have been shown to be appropriate for examining consumers' technology adoption. However, since we examine why consumers are willing to pay for privacy, we do not focus on Facebook members' *use* of the premium version, but rather on their *WTP* for privacy intention and de facto behavior. Therefore, we applied the more broadly applicable TPB to this study, which has not only been used as a theoretical framework to explain and predict individuals' behavior by numerous studies in the information systems discipline, but also provides flexibility in allowing new variables (see Venkatesh et al., 2003).

TPB assumes that "[i]ntentions to perform behaviors of different kinds can be predicted with high accuracy from attitudes toward the behavior, subjective norms, and perceived behavioral control; and these intentions, together with perceptions of behavioral control, account for considerable variance in actual behavior" (Ajzen, 1991, p. 179). Some studies have already applied the TPB in the privacy context. For instance, Lwin and Williams (2003) use a model that integrates the multidimensional development theory of privacy and TPB to examine the fabrication of information online. Furthermore, George (2004) applied TPB in an empirically tested model on internet purchasing that involved the two privacy-related constructs internet trustworthiness beliefs and unauthorized use beliefs, assuming that these constructs are the antecedents of consumers' attitude toward internet purchasing. In a more recent study, Saeri et al. (2014) applied TPB to predict Facebook users' online privacy protection, while Yao (2011) developed a hypothetical TPB-based model for the self-protection of online privacy. However, since our study examines Facebook users' WTP for privacy intention and their de facto behavior when offering them the opportunity to subscribe to a premium version of the platform, it differs visibly from prior work. We thus apply the original TPB framework to our special context. Additionally, we propose three antecedents of attitude—perceived internet privacy risk, perceived usefulness, and trust—in order to better understand the determinants that affect Facebook users' WTP for privacy. By extending the TPB, we follow an established approach that has been applied in several prior studies (e.g. Lee, 2009; Pavlou and Fygenson, 2006; Taylor and Todd, 1995a, 1995b). The research model is illustrated in Figure 1.

Antecedents of attitude

Considering the underlying privacy calculus concept, it has generally been proven that privacy risk influences consumers' privacy intentions and behaviors respectively (Li, 2011; Smith et al., 2011). In respect of our research focus, privacy risk mainly refers to consumers' uncertainty about the possible negative consequences of using content platforms, since their operators commercialize users' personal information. Previous studies have conceptualized this fear, for example, as risk beliefs (Hong and

Thong, 2013), perceived privacy risk (Dinev et al., 2013), or perceived internet privacy risk (Dinev and Hart, 2006), generally measuring "the degree to which an individual believes that a high potential for loss is associated with the release of personal information to a firm" (Smith et al., 2011, p. 1001). As a consequence, consumers might like the idea of paying for privacy in order to reduce their privacy risk when using a content platform. Accordingly, previous studies have already suggested that privacy risk is an antecedent of consumers' attitude toward privacy protection (see Saeri et al., 2014). Hence, we assume that perceived internet privacy risk (PR), which fits well with the given online context, is positively related to users' attitude (AT) toward subscribing to the privacy-enhancing premium version of Facebook:

H1. *PR is positively related to AT.*

Using a control-based definition of privacy, which we do, is a typical approach in information privacy research, specifically in the information systems discipline (see Smith et al., 2011). Even though some scholars have argued that privacy is not a form of control per se (see Smith et al., 2011), it is commonly understood as an essential factor determining privacy. For instance, Dinev et al. (2013) recently proposed a research model showing that not only perceived risk, but also perceived information control constitutes perceived privacy. Therefore, the fictional premium version of Facebook aims to enhance privacy by offering users additional privacy control features. However, with respect to the freemium revenue model, Facebook members' attitude toward subscribing to this premium version should be influenced by whether or not they conceive these features to provide added value in terms of enhancing privacy protection. Therefore, we adapt perceived usefulness (PU), known from the TAM, to this TPB-based study. This approach is strongly in accordance with previous work that has combined the TAM and the TPB to hybrid models (e.g. Lee, 2009; Taylor and Todd, 1995a), or extended the TPB by adding PU as one of several antecedents of attitude (e.g. Pavlou and Fygenson, 2006; Taylor and Todd, 1995b). Thus, we assume that:

H2. *PU is positively related to AT.*

Numerous studies, especially in the e-commerce context, have shown that not only privacy concerns and the perception of privacy risk, but also trust in an internet company are relevant factors that affect consumers' attitude toward online behaviors (e.g. George, 2004; Jarvenpaa et al., 2000; Pavlou and Fygenson, 2006). It has, moreover, been found that internet companies can build trust and, thereby, enhance consumers' WTP by signaling privacy protection, or by having a privacy seal (e.g. Mai et al., 2010; Tsai et al., 2011). Thus, trust is also expected to have an impact on users' WTP for privacy-enhancing offerings. Given the growing awareness of platform operators' commodification of personal information, Facebook members might not believe that the premium version with additional privacy control features would really impact Facebook's actual privacy practices and prevent personal data exploitation. Thus, in contrast to other studies, we do not focus on general trust in a content platform. Instead, we assume that trust (TS) in the Facebook premium version is positively related to the attitude (AT) toward subscribing to the premium version:

H3. *TS is positively related to AT.*

Theory of Planned Behavior

Furthermore, following the original TPB framework (Ajzen, 1991), we assume that attitude (AT), subjective norm (SN), and perceived behavioral control (PB) can predict users' intention (IN) to subscribe to the fee-required premium version of Facebook. AT is the degree to which a Facebook user favora-

bly or unfavorably assesses subscribing to the premium version, SN is the perceived social pressure to subscribe to the premium version, and PB is the perceived ease or difficulty of subscribing to the premium version. Finally, we expect that behavioral intention, as well as the perception of behavioral control, is positively related to de facto WTP for privacy behavior (WTPB), which is paying a fee in order to subscribe to the premium version of Facebook. While the TPB model assumes that there are additional relationships between the constructs, they are not absolutely necessary for this study's aim and were excluded to keep the model as simple as possible. Thus, we formulate the following hypotheses:

H4. *SN is positively related to IN.*

H5. *AT is positively related to IN.*

H6a. *PB is positively related to IN.*

H6b. *PB is positively related to WTPB.*

H7. *IN is positively related to WTPB.*

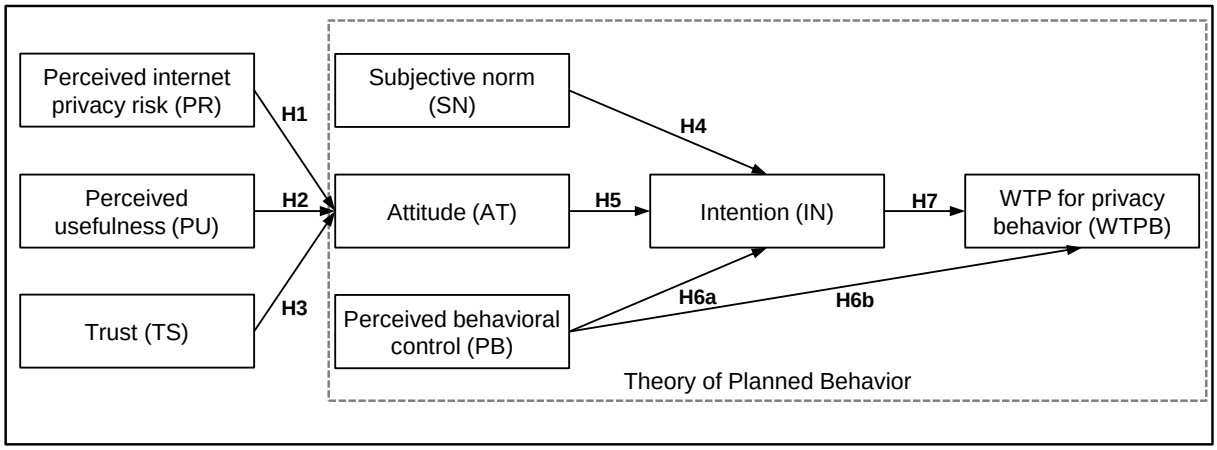

Figure 1. Research model.

3 Research Design and Data Collection

3.1 Applying the privacy-freemium model to Facebook

Offering both a free and premium version of a content platform such as Facebook falls under the freemium strategy. Freemium, coined by combining the words "free" and "premium," is a specific revenue model for earning money with internet content (Wagner et al., 2014). Applied to this study's context, freemium means that all users have access to a gratis basic version of a given content platform, which possibly generates revenues from advertising (Anderson, 2009), while additional value-added features are available for a fee (Wagner et al., 2014). With this in mind, as new approach, the freemium revenue model can be adapted to address different privacy-related user preferences. For instance, online social network providers might allow their members to use the platform's free version in exchange for utilizing their personal information, as is usually the case, but might also offer a premi-

um version with additional privacy control features in return for a monthly fee (Schreiner et al., 2013). In such situations, users can decide whether or not they are willing to pay for privacy. Hence, we adapted the idea of a privacy-freemium model in order to develop a believable scenario that is applicable for examining actual WTP for privacy behavior by using the example of Facebook, as described in the following.

Before answering the questionnaire, the participants were told that privacy issues are very relevant to content platforms, and, since privacy legislation development in Europe, particularly in Germany, is still uncertain, operators are seeking innovative solutions. Further, they were told that, since privacy issues are especially relevant for online social networks, Facebook was currently considering introducing two different types of user accounts—a regular free basic version and a new subscription-based premium version, which offers additional privacy control features for a monthly fee. Finally, the respondents were told that they had been selected to evaluate the premium version of Facebook before its possible launch.

Subsequently, the respondents were asked to look carefully at the new premium version. For this purpose, we described a fictional premium version, adapting Facebook's typical brand design, and integrating a screenshot of it into the survey. Compared to the free basic version, the new premium version offered a set of additional privacy control features based on prior work on identity management and fair information practice principles (Cranor, 2003; Hansen et al., 2008). We developed four feature categories: (1) collecting (i.e. giving users the ability to control what personal information could be collected), (2) using (i.e. giving users the ability to control the specific purposes for which personal information could be used), (3) sharing (i.e. giving users the ability to control the extent to which personal information could be shared with others), and (4) administrating (i.e. giving users the ability to look at, edit, and delete saved personal information). Each feature category contained several selection fields that the premium users could enable or disable independently in order to control their personal data utilization. These setting options take into account that Facebook users might prefer allowing particular practices (e.g. only utilizing their public personal information, using location-based information, or providing personalized advertising and recommendations), while avoiding unwanted practices (e.g. analyzing private messages, tracking consumers' online behaviors, or sharing personal information with third parties).

3.2 Scale development

In order to test the research hypotheses, the illustration of the premium version of Facebook was followed by a number of items measuring the constructs specified in the research model. Scale development was based on a review of the information privacy and TPB literature. Only validated standard scales that are appropriate to this study's aim were adapted and modified where necessary. The measuring instrument included only reflective construct measures, which were operationalized as seven-point Likert scale items. AT, IN, PB, PU, SN, and TS range from 1 (strongly disagree) to 7 (strongly agree); PR ranges from 1 (very low risk) to 7 (very high risk). All the items were translated into German. Table 1 lists the measuring instrument constructs, items, and sources. However, given the privacy paradox, a special method is required to measure the WTP for privacy behavior, which we describe below.

Constructs and items		Source
AT	Imagine that Facebook would provide the premium version at a reasonable price: To what extent do you agree with the following statements?	(Taylor and Todd, 1995b)
	AT_1 Subscribing to the premium version is a good idea.	
	AT_2 I think it is positive to subscribe to the premium version.	
	AT_3 I like the idea of subscribing to the premium version.	
	AT_4 I believe that it would be good to subscribe to the premium version.	

IN	Imagine that Facebook would provide the premium version at a reasonable price: To what extent do you agree with the following statements? IN_1 I intend to subscribe to the premium version. IN_2 I aim to subscribe to the premium version. IN_3 I plan to subscribe to the premium version.	(Venkatesh et al., 2003)
PB	To what extent do you agree with the following statements? PB_1 I would be able to subscribe to the premium version. PB_2 Subscribing to the premium version would be possible for me. PB_3 I could subscribe to the premium version without any problems.	(Taylor and Todd, 1995b)
PR	What do you believe is the risk for regular internet users due to the possibility that… PR_1 …records of transactions could be sold to third parties? PR_2 …personal information submitted could be misused? PR_3 …personal information could be made available to unknown individuals or companies without your knowledge? PR_4 …personal information could be made available to government agencies?	(Dinev and Hart, 2006)
PU	To what extent do you agree with the following statements? PU_1 Using the premium version would improve data protection on Facebook. PU_2 Using the premium version would enhance controlling personal information on Facebook. PU_3 Using the premium version would increase privacy protection on Facebook. PU_4 I find the premium version would be useful in terms of data protection on Facebook.	(Venkatesh and Davis, 1996)
SN	To what extent do you agree with the following statements? SN_1 People who influence my behavior would think that I should subscribe to the premium version. SN_2 People who are important to me would think that I should subscribe to the premium version.	(Taylor and Todd, 1995b)
TS	To what extent do you agree with the following statements? TS_1 The premium version is trustworthy. TS_2 The premium version is serious. TS_3 The premium version will keep promises it makes to me. TS_4 I believe that the premium version will impact data protection as promised. TS_5 The premium version is credible.	(Koufaris and Hampton-Sosa, 2004)

Table 1. Measuring instrument.

3.3 Measuring the willingness to pay

At the end of the survey, the participants were given the opportunity to subscribe to the premium version of Facebook, and thereby upgrade their free basic account in order to receive additional privacy control features. However, owing to the privacy paradox, which has shown cases where privacy intentions did not lead to expected behaviors (Bélanger and Crossler, 2011), we had to apply an incentive-compatible method to measure users' actual WTP for privacy behavior. Hence, we made the participants believe that they would really have to pay a fee for subscribing to the premium version. Accordingly, they were told that the price for the premium version of Facebook had not yet been determined and that it was up to them to decide whether or not, as well as how much, they wanted to pay for subscribing to the premium version for one month. They were, moreover, told that they would be able to extend their premium subscription.

However, based on the Becker-DeGroot-Marschak method (Becker et al., 1964), we told the respondents that they could only access the premium version if their bid was at least as high as an automatically generated random price, and that, if this condition was fulfilled, they would also have to pay this price. In contrast, if their bid was lower than the random price, they would not be allowed to subscribe to the premium version and would not have to pay a price. In so doing, we ensured that the survey participants would submit an offer that was in accordance with their real WTP for privacy. We had tested the WTP for privacy measuring method in a pretest before applying it to this study. To sum up, actual WTP for privacy behavior (WTPB) was measured as the amount that Facebook users are willing to pay to subscribe to the premium version with additional privacy control features, while an unwillingness to subscribe to the premium version expressed a WTP for privacy equal to zero. At the end of the survey, we debriefed the participants and informed them about the real aim of the study. Of course, respondents were also informed that they did not have to pay anything.

3.4 Survey administration and sample

Data was collected through a web-based survey of 553 German Facebook users from May 23-28, 2014. The acquisition of the participants was based on a commercial online panel and conducted with the help of a specialized online survey service provider (www.norstat.de), who selected respondents with respect to their gender and age to achieve an appropriate demographic distribution, and chose only Facebook users to participate in the study. All the participants who had completed the questionnaire received bonus points from the online panel provider which can be converted into monetary and other rewards. In order to prepare the sample for analysis, we checked the data set for outliers, and adjusted for respondents who had spent less than four minutes on answering the questionnaire, assuming that their responses were not of an adequate quality. After that, 470 responses were usable. The sample revealed an appropriate gender distribution, with 58% female and 42% male respondents. The respondents were aged between 16 and 60, and on average 40 years old. In sum, although the sample did not precisely reflect the population of German Facebook users, it was satisfactory in terms of its demographic distribution.

4 Data Analysis and Results

Since the participants could submit free bits in order to gain access to premium privacy features, WTPB ranged between a minimum of 0 euro to a maximum of 15 euro, with the analyzed observations providing an average of 0.63 euro. We applied structural equation modeling to analyze the data and test our hypotheses by means of the statistical software SmartPLS 2.0 M3 (Ringle et al., 2005), using a partial least squares (PLS) algorithm. Since PLS estimations are based on iterations of regressions, we did not have to fulfill hard sample distribution requirements, such as the normality of the distributions (Lohmöller, 1989). We used the bootstrapping algorithm to determine factor loadings and path coefficients, and to examine their significance. In addition, we used the PLS algorithm to check for cross loadings and to examine the measurement and structural model's quality. The missing value algorithm was applied to both procedures. Finally, we used blindfolding to examine the predictive relevance of our research model. We divided the data analysis's results, as presented below, into two analytic steps: First, the measurement model's quality was assessed to ensure its validity and reliability. Subsequently, we examined the research hypotheses and the overall quality of the proposed research model. We followed Hair et al. (2011) in order to check for statistical threshold values.

4.1 Measurement model

We determined the reflective measurement model's quality by examining its indicator reliability, internal consistency reliability, convergent validity, and discriminant validity. First, the factor loadings (all of which were higher than 0.7) and their statistical significance (all of which were on a level $p < 0.01$) confirmed adequate indictor reliability. Next, the composite reliability and Cronbach's α values

were higher than 0.7 and thus showed adequate internal consistency reliability. All the relevant values, as well as the descriptive statistics, are shown in Table 2.

Construct	Item	Factor loadings*	Means	Standard deviations	Means (construct)	Standard deviations (construct)	Composite reliability	Cronbach's alpha
AT	AT_1	0.970	3.573	2.000	3.596	1.982	0.987	0.982
	AT_2	0.965	3.535	2.043				
	AT_3	0.976	3.667	2.067				
	AT_4	0.984	3.610	2.031				
IN	IN_1	0.984	2.746	1.960	2.833	2.010	0.990	0.984
	IN_2	0.986	2.826	2.061				
	IN_3	0.984	2.925	2.104				
PB	PB_1	0.963	5.117	1.967	5.080	1.912	0.981	0.971
	PB_2	0.975	5.033	1.994				
	PB_3	0.978	5.089	1.942				
PR	PR_1	0.773	5.732	1.417	5.684	1.321	0.913	0.934
	PR_2	0.956	5.610	1.382				
	PR_3	0.780	5.808	1.413				
	PR_4	0.883	5.587	1.578				
PU	PU_1	0.964	4.709	1.881	4.772	1.747	0.966	0.953
	PU_2	0.874	4.977	1.755				
	PU_3	0.957	4.742	1.857				
	PU_4	0.947	4.662	1.964				
SN	SN_1	0.992	3.202	2.070	3.223	2.089	0.992	0.984
	SN_2	0.992	3.244	2.140				
TS	TS_1	0.949	4.324	1.836	4.237	1.750	0.981	0.976
	TS_2	0.970	4.319	1.804				
	TS_3	0.958	4.277	1.823				
	TS_4	0.953	4.103	1.812				
	TS_5	0.948	4.160	1.882				
WTPB	$WTPB_1$	1.000	0.632	2.091	0.632	2.091	1.000	1.000
*All loadings were statistically significant at a level $p < 0.01 = t > 2.58$.								

Table 2. Factor loadings, descriptive statistics, composite reliabilities, and Cronbach's alphas.

Regarding convergent validity, the average variance extracted (AVE) of all constructs exceeded the required threshold value of 50 percent (see Table 3). With regard to discriminant validity, we checked the latent construct correlations against the square root of the specific AVE. Since the AVE square root values were higher than the highest latent variable correlation in all cases, the Fornell-Larcker criterion (Fornell and Larcker, 1981) was also fulfilled (see Table 3). Additionally, all the items had low cross loadings (all clearly smaller than the factor loadings), also indicating adequate discriminant validity. In sum, the measurement model's quality proved to be satisfactory.

	AVE	AT	IN	PB	PR	PU	SN	TS	WTPB
AT	0.948	0.974							
IN	0.969	0.803	0.984						
PB	0.945	0.323	0.340	0.972					
PR	0.725	0.070	-0.035	0.138	0.851				
PU	0.877	0.660	0.563	0.193	0.072	0.936			
SN	0.985	0.784	0.781	0.296	0.044	0.548	0.992		
TS	0.913	0.715	0.642	0.171	-0.011	0.850	0.598	0.956	
WTPB	1.000	0.339	0.448	0.148	-0.028	0.215	0.384	0.275	1.000

The columns AT, IN, PB, PR, PU, SN, TS, and WTPB present latent variable correlations as well as square roots of AVEs (denoted in grey).

Table 3. AVE (square root) values and latent variable correlations.

4.2 Structural model

Subsequent to evaluating the measurement model, we tested our hypotheses by examining assumed path coefficients and their significance (see Figure 2). In contrast to H1, we found that PR was not significantly related to AT (t = 1.46). However, as H2 and H3 suggest, PU (β = 0.17, t = 1.83) and TS (β = 0.57, t = 5.84) were positively related to AT. Thus, we found support for H2 and H3, but not for H1. Overall, PR, PU, and TS explained 52% of the variance in AT. In addition, SN (β = 0.39, t = 5.25) and AT (β = 0.48, t = 6.55) were positively related to IN (H4, H5). We further found a weak (β = 0.07), but significant (t = 1.66), relation between PB and IN (H6a). Therefore, H4, H5, and H6a are supported; and SN, AT, and PB explained 71% of the variance in IN. In contrast, the relation between PB and WTPB was not significant at a 10% level (t = 0.25). Accordingly, H6b is not supported. Moreover, as H7 suggests, IN was positively related to WTPB (β = 0.45, t = 9.88). Finally, we explain 20% of the variance in WTPB.

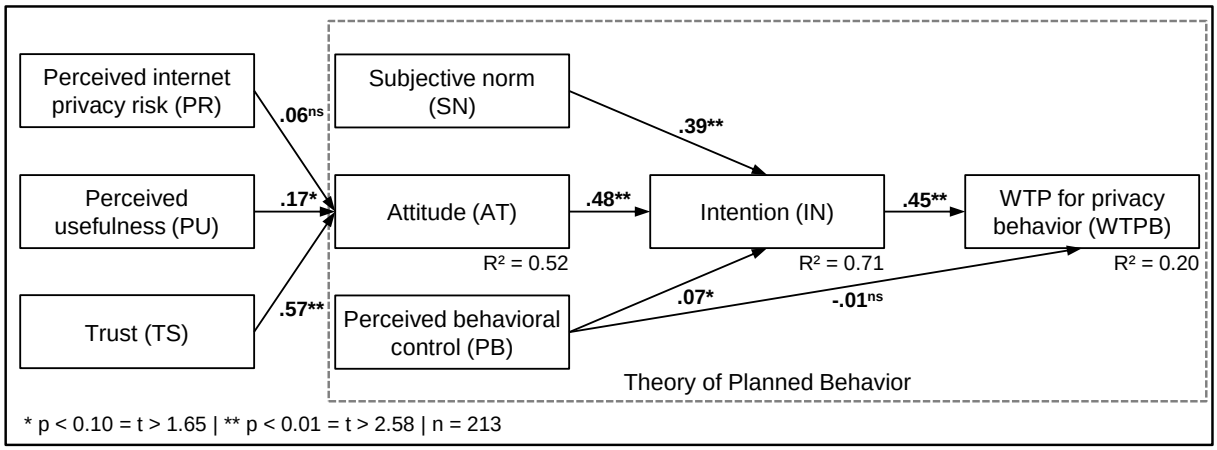

Figure 2. Tested research model.

In addition, Stone-Geisser's Q^2 was determined to assess the predictive relevance of our structural model. We conducted the blindfolding procedure to obtain cross-validated redundancy measures for all endogenous constructs. Since we found $Q^2 > 0$ for each construct ($Q^2_{AT} = 0.49$, $Q^2_{IN} = 0.67$, $Q^2_{WTPB} = 0.19$), our model's predictive relevance was proved (Hair et al., 2011).

In sum, as shown in Table 4, most hypotheses are supported. Moreover, we could account for between 20% and 71% of the variance in endogenous constructs, which is a satisfactory result when examining actual WTP for privacy behavior.

Hypothesis	Relationship	Support
1	PR (+) → AT	No
2	PU (+) → AT	Yes, level 0.10
3	TS (+) → AT	Yes, level 0.01
4	SN (+) → IN	Yes, level 0.01
5	AT (+) → IN	Yes, level 0.01
6a	PB (+) → IN	Yes, level 0.10
6b	PB (+) → WTPB	No
7	IN (+) → WTPB	Yes, level 0.01

Table 4. Overview of the tested hypotheses.

5 Conclusion

This study examined the privacy-freemium model as a new revenue model for media companies. In particular, we aimed to explain consumers' WTP for privacy when using content platforms like Facebook by applying the TPB as a theoretical framework. An innovative research design was developed, offering 553 participants of an online survey the opportunity to subscribe to a privacy-enhancing premium version of Facebook for a monthly fee. We thus designed a fictional premium version of the platform with additional privacy control features. A new TPB-based research model of the WTP for privacy was developed and proven to have high measurement quality and explanation power.

Our findings showed that perceived usefulness and trust significantly affect consumers' attitude toward subscribing to the premium version of Facebook, while perceived internet privacy risk did not have any significant impact on attitude. In accordance with the relevance of control shown in the information privacy literature (see Smith et al., 2011), the positive influence of perceived usefulness on attitude indicates that having access to additional privacy control features could provide users with added value. However, given the strong impact of trust, the attitude toward subscribing to a premium version also depends on how far Facebook members believe that premium privacy features would really impact Facebook's actual privacy practices and prevent personal data exploitation. Since we did not find a significant influence of perceived internet privacy risk, our results suggest that even consumers who are afraid of privacy violations do not assess subscribing to a platform's premium version (more) favorably if they do not perceive it as offering added value and as trustworthy.

As the TPB proposes, the more favorable users' evaluation of subscribing to the premium version, the higher their intention to do so, and also the higher their actual WTP for subscribing to the premium version. Thus, from a practical point of view, offering additional privacy control features, particularly in the form of a privacy-freemium model, might be a way for platform operators to monetize privacy protection as a new revenue model—provided that their users perceive the payable premium version as useful and trustworthy. Furthermore, considering social norm's impact on intention, there should be a level of social pressure to subscribe to the premium version if Facebook were to provide such an offer. In contrast, we found that perceived behavioral control only weakly affects intention and does not affect WTP behavior at all. Since Ajzen (1991) expects the relevance of social norm, attitude, and perceived behavioral control to vary across behaviors and situations, it is conceivable that the latter is rather insignificant in the given context. Thus, summarizing our findings, TPB was shown to be an adequate theory to examine WTP for privacy.

However, the results of prior research on WTP for privacy indicated that there is a contradiction between privacy intentions and behaviors, which is denoted as the privacy paradox (Bélanger and Crossler, 2011; Smith et al., 2011). Acquisti (2004), as well as Acquisti and Grossklags (2005), explain this phenomenon, suggesting that even individuals who really want to protect their privacy might not do so, because their privacy-related decision making is affected by bounded rationality. In contrast, our results demonstrated strong, highly significant, and predictive correlations between attitude, intention,

and actual behavior. This indicates that users who appreciate monetizing privacy protection instead of having their personal information commercialized would be willing to pay a price premium when using content platforms. One of the reasons for our findings differing from those of prior research might be our use of the applied freemium approach. Since subscribing to a premium version of Facebook would provide an upgraded service with new privacy control features, users might perceive privacy protection as an additional value and, thus, be more willing to pay for it.

In sum, we have shown that consumers are willing to pay for privacy, provided they perceive the premium version as offering added value and as trustworthy. Our results have implications for media companies aiming to monetize privacy protection in the form of a privacy-freemium model: First, platform operators have to develop and implement privacy premium features that really enhance users' possibilities to control and adjust their personal information's (commercial) exploitation; such operators therefore need to achieve sufficient differences between the free and premium version (see Wagner et al., 2014). Second, platform operators should take steps to enhance consumers' trust in a premium version, such as investing in marketing operations (e.g. launching an information campaign that increases transparency by explaining the differences between the free and premium version) or allowing independent third parties (e.g. privacy organizations and initiatives, privacy seal programs, and data protection authorities) to verify the privacy protection. However, this study also has limitations. While we could explain 71% of the variance in intention, we could only explain 20% of the variance in WTP for privacy behavior. Although this is a satisfactory explanation power when examining actual behaviors, the privacy paradox cannot be completely denied. Other (moderating) factors that were not taken into account in our model might also play a relevant role in WTP for privacy. Moreover, we investigated consumers' WTP for privacy using the example of the online social network Facebook, which contains a large volume of personal information and is thus highly relevant in terms of privacy issues. However, we were unable to confirm our results' generalizability. Thus, further research is necessary on WTP for privacy in terms of different types of platforms (e.g. search engines or opinion portals).

References

Acquisti, A. (2004). "Privacy in Electronic Commerce and the Economics of Immediate Gratification." In: *Proceedings of the 5th ACM Conference on Electronic Commerce (EC)*. New York: USA, 21–29.

Acquisti, A. and J. Grossklags (2005). "Privacy and Rationality in Individual Decision Making." *IEEE Security & Privacy* 3 (1), 26–33.

Acquisti, A. and H. R. Varian (2005). "Conditioning Prices on Purchase History." *Marketing Science* 24 (3), 367–381.

Ajzen, I. (1991). "The Theory of Planned Behavior." *Organizational Behavior and Human Decision Processes* 50 (2), 179–211.

Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Monterey: Brooks/Cole Publishing.

Anderson, C. (2009). *Free. The Future of a Radical Price*. London: Random House Business Books.

Becker, G. M., DeGroot, M. H. and J. Marschak (1964). "Measuring Utility by a Single-Response Sequential Method." *Behavioral Science* 9 (3), 226–232.

Bélanger, F. and R. E. Crossler (2011). "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems." *MIS Quarterly* 35 (4), 1017–1041.

Beresford, A. R., Kübler, D. and S. Preibusch (2010). *Unwillingness to Pay for Privacy: A Field Experiment*. IZA DP No. 5017. URL: http://ftp.iza.org/dp5017.pdf (visited on 3/16/2014).

Chellappa, R. K. and R. G. Sin (2005). "Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma." *Information Technology and Management* 6 (2-3), 181–202.

Chyi, H. I. (2012). "Paying for What? How Much? And Why (Not)? Predictors of Paying Intent for Multiplatform Newspapers." *International Journal on Media Management* 14 (3), 227–250.

Cranor, L. F. (2003). "'I Didn't Buy it for Myself'. Privacy and Ecommerce Personalization." In: *Proceedings of the 2003 ACM Workshop on Privacy in the Electronic Society (WPES).* Washington: USA, 111–117.

Culnan, M. J. and R. J. Bies (2003). "Consumer Privacy: Balancing Economic and Justice Considerations." *Journal of Social Issues* 59 (2), 323–342.

Davis, F. D., Bagozzi, R. P. and P. R. Warshaw (1989). "User Acceptance of Computer Technology: A Comparison of two Theoretical Models." *Management Science* 35 (8), 982–1003.

Dinev, T. and P. Hart (2006). "An Extended Privacy Calculus Model for E-Commerce Transactions." *Information Systems Research* 17 (1), 61–80.

Dinev, T., Xu, H., Smith, H. J. and P. Hart (2013). "Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts." *European Journal of Information Systems* 22 (3), 295–316.

Egelman, S., Felt, A. P. and D. Wagner (2013). "Choice Architecture and Smartphone Privacy: There's a Price for That." In: Böhme, R. (Ed.). *The Economics of Information Security and Privacy*. Heidelberg: Springer, 211–236.

Fornell, C. and D. F. Larcker (1981). "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error." *Journal of Marketing Research* 18 (1), 39–50.

George, J. F. (2004). "The Theory of Planned Behavior and Internet Purchasing." *Internet Research* 14 (3), 198–212.

Gomez, J., Pinnick, T. and A. Soltani (2009). *KnowPrivacy*. UC Berkeley, School of Information. URL: http://www.knowprivacy.org/report/KnowPrivacy_Final_Report.pdf (visited on 3/16/2014).

Grossklags, J. and A. Acquisti (2007). "When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information." In: *Proceedings of the 6th Workshop on the Economics of Information Security (WEIS 2007).* Pittsburgh: USA.

Hair, J. F., Ringle, C. M. and M. Sarstedt (2011). "PLS-SEM: Indeed a Silver Bullet." *Journal of Marketing Theory and Practice* 19 (2), 139–151.

Hann, I.-H., Hui, K.-L., Lee, S.-Y. T. and I. P. L. Png (2007). "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach." *Journal of Management Information Systems* 24 (2), 13–42.

Hansen, M., Schwartz, A. and A. Cooper (2008). "Privacy and Identity Management." *IEEE Security & Privacy* 6 (2), 38–45.

Hess, T. (2014). "What is a Media Company? A Reconceptualization for the Online World." *International Journal on Media Management* 16 (1), 3–8.

Hong, W. and J. Y. L. Thong (2013). "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies." *MIS Quarterly* 37 (1), 275–298.

Jarvenpaa, S. L., Tractinsky, N. and M. Vitale (2000). "Consumer Trust in an Internet Store." *Information Technology and Management* 1 (1-2), 45–71.

Kobsa, A. (2007). "Privacy-Enhanced Web Personalization." In: Brusilovsky, P., Kobsa, A. and W. Nejdl (Eds.). *The Adaptive Web. Methods and Strategies of Web Personalization*. Berlin: Springer, 628–670.

Koufaris, M. and W. Hampton-Sosa (2004). "The Development of Initial Trust in an Online Company by New Customers." *Information & Management* 41 (3), 377–397.

Krasnova, H., Hildebrand, T. and O. Günther (2009). "Investigating the Value of Privacy in Online Social Networks: Conjoint Analysis." In: *Proceedings of the 30th International Conference on Information Systems (ICIS).* Phoenix: USA, Paper 173.

Krasnova, H., Kolesnikova, E. and O. Günther (2010). "Leveraging Trust and Privacy Concerns in Online Social Networks: An Empirical Study." In: *Proceedings of the 18th European Conference on Information Systems (ECIS).* Pretoria: South Africa, Paper 160.

Lee, M.-C. (2009). "Predicting and Explaining the Adoption of Online Trading: An Empirical Study in Taiwan." *Decision Support Systems* 47 (2), 133–142.

Li, Y. (2011). "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework." *Communications of the Association for Information Systems* 28 (1), 453–496.

Lohmöller, J.-B. (1989). *Latent Variable Path Modeling with Partial Least Squares*. Heidelberg: Physica.

Lopes, A. B. and D. F. Galletta (2006). "Consumer Perceptions and Willingness to Pay for Intrinsically Motivated Online Content." *Journal of Management Information Systems* 23 (2), 203–231.

Lwin, M. O. and J. D. Williams (2003). "A Model Integrating the Multidimensional Developmental Theory of Privacy and Theory of Planned Behavior to Examine Fabrication of Information Online." *Marketing Letters* 14 (4), 257–272.

Mai, B., Menon, N. M. and S. Sarkar (2010). "No Free Lunch: Price Premium for Privacy Seal–Bearing Vendors." *Journal of Management Information Systems* 27 (2), 189–212.

Norberg, P. A., Horne, D. R. and D. A. Horne (2007). "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors." *The Journal of Consumer Affairs* 41 (1), 100–126.

Pavlou, P. A. and M. Fygenson (2006). "Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior." *MIS Quarterly* 30 (1), 115–143.

Ringle, C. M., Wende, S. and A. Will (2005): *SmartPLS. Version 2.0 (beta)*. Hamburg: Germany. URL: http://www.smartpls.de (visited on 3/31/2014).

Saeri, A. K., Ogilvie, C., La Macchia, S. T., Smith, J. R. and W. R. Louis (2014). "Predicting Facebook Users' Online Privacy Protection: Risk, Trust, Norm Focus Theory, and the Theory of Planned Behavior." *The Journal of Social Psychology* 154 (4), 352–369.

Schreiner, M., Hess, T. and F. Fathianpour (2013). "On the Willingness to Pay for Privacy as a Freemium Model: First Empirical Evidence." In: *Proceedings of the 21st European Conference on Information Systems (ECIS)*. Utrecht: Netherlands, Paper 30.

Smith, H. J., Dinev, T. and H. Xu (2011). "Information Privacy Research: An Interdisciplinary Review." *MIS Quarterly* 35 (4), 989–1015.

Taylor, S. and P. A. Todd (1995a). "Assessing IT Usage: The Role of Prior Experience." *MIS Quarterly* 19 (4), 561–570.

Taylor, S. and P. A. Todd (1995b). "Understanding Information Technology Usage: A Test of Competing Models." *Information Systems Research* 6 (2), 144–176.

Toch, E., Wang, Y. and L. F. Cranor (2012). "Personalization and Privacy: A Survey of Privacy Risks and Remedies in Personalization-Based Systems." *User Modeling and User-Adapted Interaction* 22 (1-2), 203–220.

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

Venkatesh, V. and F. D. Davis (1996). "A Model of the Antecedents of Perceived Ease of Use: Development and Test." *Decision Sciences* 27 (3), 451–481.

Venkatesh, V., Morris, M. G., Davis, G. B. and F. D. Davis (2003). "User Acceptance of Information Technology: Toward a Unified View." *MIS Quarterly* 27 (3), 425–478.

Venkatesh, V., Thong, J. Y. L. and X. Xu (2012). "Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology." *MIS Quarterly* 36 (1), 157–178.

Wagner, T. M., Benlian, A. and T. Hess (2014). "Converting Freemium Customers from Free to Premium – The Role of the Perceived Premium Fit in the Case of Music as a Service." *Electronic Markets* 24 (4), 259–268.

Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum.

Yao, M. Z. (2011). "Self-Protection of Online Privacy: A Behavioral Approach." In: Trepte, S. and L. Reinecke (Eds.). *Privacy Online. Perspectives on Privacy and Self-Disclosure in the Social Web*. Heidelberg: Springer, 111–125.