Privacy as a Part of the Preference Structure of Users App Buying Decision

Christoph Buck[1], Florian Stadler[2], Kristin Suckau[3], and Torsten Eymann[1]

[1] Chair of Information Systems Management, Bayreuth, Germany
{christoph.buck, torsten.eymann}@uni-bayreuth.de
[2] zeb – 360° Consulting for Financial Services
{florian.stadler}@zeb.de
[3] Chair for Innovation and Dialogue Marketing
{kristin.suckau}@uni-bayreuth.de

Abstract. Information privacy and personal data in information systems are referred to as the 'new oil' of the 21st century. The mass adoption of smart mobile devices, sensor-enabled smart IoT-devices, and mobile applications provide virtually endless possibilities of gathering users' personal information. Previous research suggests that users attribute very little monetary value to their information privacy. The current paper assumes that users are not able to monetize their value of privacy due to its abstract nature and non-transparent context. By defining privacy as a crucial product attribute of mobile applications the authors provide an approach to measure the importance of privacy as part of users' preference structure. The results of the conducted choice-based conjoint Analysis emphasize the high relevance of privacy in users' preference structure when downloading an app and provide an interesting contribution for theory and practice.

Keywords: Information Privacy, Personal Data, Product Attribute, Preference Structure, Mobile Applications.

1 Introduction

With the disruptive innovations of e.g. the iPhone and the iPad software in the form of mobile applications (apps) diffused in the everyday life of users. Apps are integral to the functioning of Smart Mobile Devices (SMD) like smartphones or tablets and are key elements for the interface design and functionality. Apps can be interpreted as the embodiment of ubiquitous computing, i.e. the creation of environments saturated with computing and communication capability, integrated with human users [1]. While ubiquitous computing focuses on hardware components, today's apps are the logical consequence of experiential computing; the "digitally mediated embodied experiences in everyday activities through everyday artifacts with embedded computing capabilities" [2].

At the same time, this development has considerably contributed to the emergence of a new user type of information systems. These new users integrate apps into their

13th International Conference on Wirtschaftsinformatik,
February 12-15, 2017, St. Gallen, Switzerland

Buck, C.; Stadler, F.; Suckau, K.; Eymann, T. (2017): Privacy as a Part of the Preference Structure of Users App Buying Decision, in Leimeister, J.M.; Brenner, W. (Hrsg.): Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017), St. Gallen, S. 792-806

everyday lives, which leads to fundamental changes concerning how users interact with computing devices and systems [3].

However, this excessive level of integration does not come without consequences. Many business models are based on the user data collected by SMD, which grants the marketing industry the access to exceptionally valuable information about current and potential customers [4]. Thanks to the mechanics and the real life integration of modern information systems, the value of user data is unique. Thus, users' privacy, increasingly gets at risk.

Given the fact that users' information privacy is a major part of the economic exchange when downloading apps, privacy, and the corresponding settings, have to be determined as an attribute of the value proposition of apps. In order to understand users' concerns and clearly define the necessity of user data protection, it is crucial to determine the value of privacy for users. Caused by the (perceived) abstract nature of personal data and privacy, the current paper states that users are not able to value personal data and privacy in a monetary amount. Consequently, this paper targets users' preference structures when downloading apps. With this in mind, we formulate the following research question:

- Does the protection of privacy, when downloading an app, represent a crucial product attribute for the user?

To answer this research questions, two examinations were conducted both reflecting the importance of privacy as an important attribute when purchasing an app. The HB-based utility value and the estimations of the CBC, show significantly high levels of importance for privacy. In fact, privacy is on first-place in both rankings. The remainder of this article is structured as follows: in the subsequent section, we lay out the groundwork for the definition of privacy as a value and its measurement. Following this, we will describe the methodology conjoint analysis, present our choice based conjoint analysis and its key findings. Finally, we will discuss our findings, address some limitations and conclude with suggestions for further research.

2 The Value of App Privacy

2.1 Information Privacy in the Context of Mobile Applications

Since privacy is addressed in many fields of social sciences and different definitions are used in various areas of everyday life it lacks a holistic definition [4, 5]. First of all, physical and information privacy have to be distinguished. Physical privacy relates to the "access of an individual and/or the individual's surroundings and private space" [4]. Contrary, information privacy only refers to information that is individually identifiable or describes the private informational spheres of an individual. Although information privacy is rooted in the fundamental concept of physical privacy, both are subsumed under the term of "general privacy" [4].

Even though privacy has developed and changed drastically over the last decades, Westin's definition from 1967 still holds true: information privacy is defined as "the claim of an individual to determine what information about himself or herself should

be known to others" [6]. Following Westin, 'control' is construed as an instrument of the protection of privacy, that privacy itself is often defined as the control over personal information [5]. Consequently, in this paper information privacy is defined as the ability to control the acquisition and use of one's personal information [7].

As the "pocket knife of communication" [8], SMD possess a vast amount of connected sensors, devices, and functions. SMD in combination with apps are the most common user interface to merge the broad opportunities given by the connected sensors and devices. Throughout these functions, the possibilities of gathering personal data are virtually endless. Future prospects in relation to these applications promise even more opportunities to expand data collection and immediate analysis of data. Regarding data quality, recent developments in mobile technology and an ever-increasing digitization of everyday tasks, lead to an unprecedented precision of continuously updated and integrated personal data, which is generated within mobile ecosystems like iOS and Android [9]. Consequently, apps, as the most common user interface for digitized solutions (e.g., smart services, smart homes, wearables, etc.), layer everyday activities and lives in a digital way; or how Clarke rephrased it: "Cyberspace is invading private space" [10].

In app markets, users are able to control their privacy disclosure during the purchasing process. Thus, users can actively control their disclosure of personal data and the grasping of privacy from third parties [11].

2.2 The Value of App Privacy

Dinev and Hart [12] stated that privacy "is a highly cherished value, few would argue that absolute privacy is unattainable." Privacy as digital personal information and highly personalized data collected via apps has a huge economic value [13]. With the description of personal data as a new asset class, the World Economic Forum [14] is in line with the argumentation of many researchers [4, 15]. Derived from the perspective of personal data and privacy as a commodity [16], many researchers conceive privacy as a tradeable good or asset [15]. According to this view, privacy is no longer an absolute societal value, but has an economic value, which leads to the possibility of a cost-benefit trade-off calculation made by individuals or a society [4].

Nevertheless, the authors of this article argue that privacy cannot be seen as an economic value with (for users) available market prices. First, users' distortion regarding the valuation of their own information privacy is caused by the nature of data collection, aggregation and secondary use of app markets [17]. Following Flender and Müller [18], apps are data-centric services and value is generated on different levels: e.g. between the user and the app provider, the aggregated value of the app as data centric service, and the aggregated data from various apps and underlying ecosystems by third parties [19]. As a result, in app markets it is not possible for users' to reliably evaluate their value of privacy in the moment of releasing personal information. However, major parts of the resulting costs of releasing personal informatio arise by the access, use and transfer of the data on multiple levels. Third parties (e.g., retailers, advertisers, and insurance companies) could, for instance, use that information for issues like price discrimination, advertising or risk surcharges [15]. Accordingly, the

value of users' privacy is originated in the release of the information but realized in a sphere, which cannot be controlled by the initial owner (user). In addition, users are often not aware of the possibilities of collection, aggregation and analyzation of digital information [15].

Taking the paradigm of experiential computing into account, the value of privacy increases with the (perceived) invisibility of the connected devices. With the increasing everyday life integration, devices and sensors become more and more invisible but are an increasingly self-evident part of users' daily routine. Because of the establishment in users most intimate privacy sphere, users' awareness regarding their information privacy is affected in a paradox way. In the end, privacy is perceived subjective and individually and the value of different information types and spheres is abstract and intangible. Following these arguments, the presented paper defines privacy as an abstract value. Consequently, users are not able to evaluate the monetary value of their information privacy.

2.3 Related work

When the measurement of the (perceived) value of consumers' information privacy is observed the theory of the privacy calculus has to be considered [20]. Therefore, users are supposed to undertake an anticipatory, rational weighing of risks and benefits when confronted with the decision to disclose personal information [21, 22] or conduct transactions [23]. The privacy calculus model assumes a correct and objectified understanding of the monetary value of privacy and therewith a tangible willingness to pay for privacy of the users [24, 25]. IS privacy research focused on the marketing-based concept of willingness-to-accept (WTA) and willingness-to-pay (WTP) [15]. Although asymmetries and disparities between WTA and WTP have been observed, both concepts are well established in academic research and have been applied to the topic of personal user data multiple times [15, 26]. Besides those disparities and the fact that the ownership of privacy control rights remains difficult to define in the context of apps, WTA and WTP are based on the user's perceived value for privacy and the purchased good or service. As stated above, users are indeed not able to evaluate the monetary value of their privacy, which leads to the impossibility to define the perceived value and thereby the needed maximization or reservation price for WTA or WTP. In the light of the definition of privacy as an abstract value studies which directly elicit users' valuation of privacy in survey settings gain distorted results [27–30] (see for an overview [31]). This is also described by the well-observed phenomena of the privacy paradox [24], which claims that individuals value privacy less than stating in studies and polls. It has been subject of various research in the field of information privacy, but there is no comprehensive explanation why individuals show this paradoxical behavior [24]. Consequently, WTA or WTP do not offer an adequate set of instruments to measure users' privacy concerns or the value they assign to their privacy.

Stemming from that, we recommend the approach of a choice-based conjoint analysis (CBC) to examine users' preference structure when purchasing an app. Some studies measured the preference structure as a proxy for the willingness-to-pay for privacy. Most of these studies are desktop driven and focus on the disclosure on web-

sites and online social networks [31–33] or social app adoption [34]. Despite the increasing studies applying decomposition methods there is no investigation of privacy as a stand-alone product attribute correlated with the provided functionality of the app. Therefore, a CBC is provided which outlines privacy on equal terms to other attributes like price. Hereby we are able to determine if the user only states that he values privacy or if he actually does value it in real life purchase decisions.

Accordingly, a high evaluation of privacy can be assumed when privacy is seen as a crucial product attribute of apps. Therefore, privacy has to be an important product attribute in users' preference structure when buying apps. A well-known and established methodological approach for measuring users' preferences is the Conjoint Analysis (CA). CA is an individual analysis based on the observed evaluation behavior of one specific individual [35]. The observed behavior is used to define a preference, which is a one-dimensional indicator of individual's preference structure [36]. The structure describes what object is favored by the individual. While compositional methods ask individuals about their preference for certain attributes and compose an overall judgment from it, decomposition methods, such as the CA, calculate the partial utility values for each attribute from the overall judgement of the participants [36].

3 Empirical Study

3.1 Methodological Approach

In the current study the choice-based conjoint analysis (CBC) was chosen because of its methodological and practical strengths [37]. CBC is based on the work of Louviere and Woodworth from 1983 [38] and combines the discrete choice analysis (DCA) with the Traditional Conjoint Analysis (TCA) [37]. Therefore, it is measuring population's utility functions. Those functions are estimated by representative utility functions. First, the most important assumptions are that participants always choose the product profile with the highest individual utility. Thus, it is possible to draw conclusions from the purchase decisions and the utility functions of the users [37]. Second, it is assumed that the utility function consists of a deterministic and a stochastic component, which are summed up. The main difference between CBC and TCA is that instead of ranking stimuli, the CBC wants its participants to rank different choice tasks. Those options consist of a product with a bundle of chosen attributes and their levels [37]. Instead of ranking different profiles against each other like TCA, participants have to perform fictitious purchase decisions [39]. Those choice tasks consist of the predetermined product profiles (choices) that display the attributes and their levels [37]. In the current paper a CBC following the steps of Backhaus et al. [40] was designed: definition of stimuli, design choice situation, utility model, choice model, and estimation of utility values. The CBC proves to avoid the distortions in surveys caused by group dynamics and social desirability. The advantages of the indirect measurement of preferences for certain product attributes utilizing the CBC approach shine especially against the background of the privacy paradox.

3.2 Survey Design

Apps where chosen as research objects, due to their broad diffusion in mass user markets and their everyday life integration. To ensure participants common understanding regarding e.g. functionality, provider, and the privacy level of access privileges an appealing CampusApp was defined and conducted at a German university. The functionality of the app was designed similar to campus apps of comparable universities (navigation on campus, information about public transportation, library services, organization of studies incl. online platform of the university, food on campus, university sports programs).

To keep a low stress level for the study participants, the number of attributes was set to four. To determine the attributes, different steps were conducted. First, the recent literature about apps' product attributes, as well as their assigned categories and their influence to the users' decision-making process when purchasing an app were analyzed [41]. Second, a word-frequency text analysis of 73 apps from the categories 'most popular' and 'top 10' apps with and without a purchase price was performed. In the third step the available types of information in the two most common app stores (Android Play Store and Apple App Store) were examined. Their separate information was compared to one another, as well as categorized into five different groups. With the broad variety of app product attributes, an online survey (N=151) to estimate the perceived importance of the different information types was conducted and narrowed down to a suitable amount of four attributes for the CBC. Attributes and levels are shown in table 1.

Table 1. App Attributes and Levels by Groups

Groups	Level 1	Level 2	Level 3
I - Price	0,00 €	0,99 €	2,77 €
II - Privacy	Only functionally required permissions requested with privacy policy	More than functionally required permissions requested with privacy policy	More than functionally required permissions requested without privacy policy
III - Rating	4 stars	3 stars	2 stars
IV - App	0-500 MB	500 MB - 1 GB	> 1 GB

The attribute's levels of the price group (I) were defined by taking a closer look at the common prices in the app stores. With over 60% of all apps since 2009, the price of 0,00 € is by far the most common [42]. Although the average app price is reported between $1.13 [43] and $1.91 [44] by different sources, researchers agree that this price is decreasing. Following, and to design an attractive price in the middle for the second level, 0,99€ was determined. In order to create a realistic high-end price, the price of 2,77€ was chosen. This price is based on a bidding game for a messenger app by Buck [45].

In the privacy-related group (II), the handling of personal user data and the technical access to personal user data were combined into one attribute. Taking a closer look at the current handling of personal user data, Sunyaev, Dehling, Taylor, and Mandl's [46] work shows that only 30.5% of the examined mobile health apps had a privacy policy. Additionally, and since advertising is one of the most used mobile app monetization models of developers [47], apps frequently request more technical access and permissions than they actually need to function properly. Based on those findings, only the first level of privacy was designed to request the required amount of permissions and a privacy policy. The other two levels both requested more technical permissions than necessary. The difference between those last two levels is that the second level possesses a privacy policy, but the third level does not. In the survey itself, required permissions were displayed with an exemplary set of functionally required permissions and an exemplary set of permissions which exceed the functionally required amount and permission types significantly. Both sets were modeled on the basis of permission groups given in the Android OS, which are very similar to the ones in the iOS.

Within the app ratings group (III), the average rating in stars was the only attribute reaching a Likert-scale average above five. Although rankings and ratings in the app stores have proven to suffer from fraud [48], based on the pre-study, app users are familiar and relying on the star ratings. Following, the levels for average app rating in stars were determined to two, three, and four stars. Zero stars and five stars were not considered because those ratings mostly consist of as little as one review or none at all.

In the last considered group of directly app-related information attributes (IV), the 'compatibility with own devices' was the most important attribute. Due to the fact that this is certainly a deal-breaker attribute for users [35], the second most important attribute was chosen for that group: needed size on device in MB/GB. Since there are all kinds of different apps, the levels were set to <500 MB, 500 MB -1 GB and >1 GB.

To avoid the phenomenon of forced choice and to design the choice situation as realistic as possible, an additional 'none' option is included [40]. Additionally, an unrealistic set containing level one of price and privacy were not included to ensure a realistic choice situation for the participants. With the four chosen attributes their three levels, a total of 81 different stimuli sets are possible. The stimuli were presented in the form of virtual cards with descriptions.

In order to match the recommended range, a fractional design with 10 randomized stimuli and two fixed stimuli was chosen. Based on the recommended number of choices per set of $K \leq 7$ [40], four randomized choices and a 'none' option were chosen for the CBC. The fixed choice tasks were designed to confront the participants with a trade-off situation between price and privacy, as shown in figure 1.

In choice 1 and 3, the attributes of rating and app-related are both marked as level 1. The difference between those two options is to be found in the attributes of price and privacy. Choice 1 has a level 1 privacy scheme, but a level 3 price (2,77€). Choice 3 has a level 1 price (0,00€), but a level 3 privacy scheme. Choice 2 and 4 are designed to be middle-class options with level 2 compositions for price and privacy. Nevertheless, choice 2 is dominated by choice 4, since it is shaped significantly worse in the rating and size attributes. With four attributes and three levels each in a choice situation with a choice set of four plus a 'none' option, so-called overlaps occur in every

single choice set. These overlaps allow improvement in the measurement of precise interactions between the attributes [49]. Still, and in order to prevent impacts that are too drastic on the main effects, the balanced overlap was chosen as task generation method [49]. Since the recommended range of choice tasks is 8 to 20 and the participants' concentration decreases significantly with every choice task [50], only 10 randomized choice tasks were displayed.

Durchschnittliche Bewertung	★★★☆☆	★★☆☆☆	★★☆☆☆	★★★★★	
Datenschutzerklärung und Berechtigungen	Datenschutzerklärung vorhanden **Berechtigungen** - Identität - Standort - Telefon - Fotos, Medien und Dateien - Sonstige	Datenschutzerklärung vorhanden **Berechtigungen** - Identität - Geräte und App-Verlauf - Kalender - Standort - Telefon - Fotos, Medien und Dateien - Geräte-ID und Anrufinformationen - Sonstige	Datenschutzerklärung **nicht** vorhanden **Berechtigungen** - Identität - Geräte und App-Verlauf - Kalender - Standort - Telefon - Fotos, Medien und Dateien - Geräte-ID und Anrufinformationen - Sonstige	Datenschutzerklärung vorhanden **Berechtigungen** - Identität - Standort - Telefon - Fotos, Medien und Dateien - Sonstige	KEINE: Ich würde keine der Alternativen wählen.
Benötigter Speicherplatz in MB/GB	500 MB - 1 GB	> 1 GB	500 MB - 1 GB	0 - 500 MB	
Kaufpreis	2,77 €	2,77 €	0,99 €	0,99 €	
	○	○	○	○	○

Figure 1. Exemplary Random Choice Set with Four Stimuli

3.3 Data Collection

The CBC was conducted via an online survey using Sawtooth Software. Since the study was conducted at a German university, all questions were presented in German only. At the beginning of the study, a skip logic question was given with the aim to select only participants with ties to this specific university. This was established to ensure a minimum involvement regarding the usage and functionalities were given and the incentive for downloading the CampusApp was comparable. Following, the participants were asked technical context information (e.g. SMD usage, on-device installed apps, app downloading habits, and buying likelihood of apps in the near future). Afterwards, the participants were asked to rank six different attributes according to their importance when considering to download an app. In order to introduce the CBC, the CampusApp was explained with an image and a list of functions. A second explanation including how the following choice sets will look and introductions for the CBC were displayed on next screen.

As outlined before, the CBC itself consists of 10 randomized, as well as two fixed, choice tasks. The fixed choice tasks were designed to examine a direct trade-off between price and privacy, as well as to conduct a hold-out analysis to predict the prognosis validity. After the CBC, participants were asked for their gender, age, and the brand of their SMD.

In total, 221 respondents participated in the online survey. However, 71 responses were incomplete and therefore excluded from the analysis. The participants who reported having no existing relationship to the university in the skip logic question were part of

this exclusion as well. Additionally, all participants who answered more than 50% 'none' in the choice tasks were also eliminated. This step was conducted in order to reduce the weakening impact of the attribute utility values and their levels. In total, the results of 111 responses were analyzed.

3.4 Results

Out of the 111 participants who partook in the survey, 43% were female and 57% were male. The average age (mean value) of all participants was 24.99 years. The participants were asked to rank six different attributes by importance when purchasing an app (Table 2). In order to prevent the participants from focusing on any one specific attribute and eventually influencing their answering behavior later, two additional attributes were included in the conscious priority ranking: Vendor's Reputation and Number of Ratings.

Table 2. Priority Ranking

Attribute	Rank 1	Rank 2	Rank 3	Rank 4	Rank 5	Rank 6
Reputation	8,11%	29,73%	0,90%	48,65%	9,01%	3,60%
Av. Rating	10,81%	36,04%	15,32%	16,22%	16,22%	5,41%
No. of Ratings	12,61%	15,32%	24,32%	16,22%	19,82%	11,71%
Price	17,12%	14,41%	20,72%	10,81%	23,42%	13,51%
Privacy	30,63%	2,70%	18,92%	7,21%	23,42%	17,12%
Space	20,72%	1,80%	19,82%	0,90%	8,11%	48,65%

Ranked with just over 30%, most participants named privacy as rank 1. Privacy is followed on rank 1 by required space (MB/GB) with 20.72% and price with 17.12%. In rank 2, average rating with 36.04%, vendor's reputation with 29.73%, and number of ratings with 15.32% was valued most. Based on those consciously rated importance rankings, the first indication for privacy's crucial status among app product attributes occurs.

Based on the choices made by the participants in the CBC section of the online survey, average utilities for each level of each attribute were calculated by using Sawtooth Software. As for analysis type, Hierarchical Bayes (HB), the go-to standard for utility estimations in CBC, was chosen. In total, a number of 20,000 iterations were used. Hereby, only the second 10,000 iterations were used to avoid assuming convergence too early.

As a result, utility values and standard deviations for all attributes' levels, as well as the 'none' option, are calculated (Table 3). At first sight, the negative impacts of the third levels of each attribute are noticed. In contrast to that, the first and second levels of all attributes have a positive impact on the individuals' utility values. Nevertheless, it is not possible to tell how much more or less importance an attribute or its levels have while solely regarding absolute utility values. Therefore, the average importance of each attribute is calculated in percentages based on the relative utility ranges (Table 4).

Table 3. Average Utilities (Zero-Centered Diffs)

Attributes' Levels	Average Utilities	SD
4 stars	52.25	32.13
3 stars	8.75	8.63
2 stars	-61.00	29.65
Permissions (functional) & privacy policy	52.11	46.28
Permissions (more) & privacy policy	16.25	18.83
Permissions (more) & no privacy policy	-68.36	41.65
0 - 500 MB	6.23	14.63
500 MB - 1 GB	6.57	11.90
> 1 GB	-12.80	12.04
0,00 €	53.36	34.80
0,99 €	10.40	14.44
2,77 €	-63.76	33.27
NONE	24.67	47.74

Taking a closer look at the 'Average Importance', privacy turns out to be the most important attribute with over 32%. Closely after privacy follows price with just over 30%. On the third position sits average rating with nearly 29%. With around 8%, required space (in MB/GB) is least important.

Table 4. Average Importance

Attributes	Average Importance	SD
Average Rating	28.92	14.27
Permissions & Privacy Policy	32.80	18.38
Required Space (MB/GB)	8.06	4.40
Price	30.21	15.41

Comparing the results of the consciously ranked attributes and the CBC-based results of the HB estimation for attribute importance, privacy is named as the most important attribute when buying an app in both cases. Privacy is reported as rank 1 priority with over 30% in the direct ranking question, as well as calculated as most important through the CBC's utility estimations.

Although required space is named second-important in the priority ranking, the importance percentage of only 8% shows that users do not actually value this attribute as much as they state. Price, with 17.12% is third-ranked in the priority ranking. The importance of this specific attribute is validated by the results of the CBC's HB estimation. With over 30%, price's importance is second-placed. Additionally, average rating is ranked most important on rank 2 in the priority rating. The importance, slightly below privacy and price, is to be found in the percentages of the HB estimation as well.

Tests show high values for face validity, intern validity, and prognosis validity [51]. The hit rate of 68.47% indicates decent results for the study. The study's average root likelihood is 0.6 which proves an accurate internal validity. The hit rate of 76.58% is

significantly bigger than 20% which shows a promising prognosis of validity for the study.

4 Privacy as a Crucial Product Attribute

Concluding, the results of both examinations of the attributes' importance through the priority ranking, as well as the HB-based utility value and importance estimation of the CBC, show significantly high levels of importance for privacy. In fact, privacy is on first-place in both rankings. Following the research question of whether or not privacy in the area of SMD and SMA represents a crucial product attribute for the user, must be affirmed. The fact that privacy ranks even more important than price in the consciously answered priority ranking, as well as in the CBC, shows an exceptional observation. Especially the result that privacy is ranked as no. 1 in the preference structure provides novel insights in users' intention when downloading apps. In contrast to many WTP-studies, where users were only willing to pay a very small amount of money for their privacy, the results of the conducted CBC suggest that there is a high preference for controlling privacy. This could indicate that users are willing to pay a higher purchase price than they currently do, when their privacy protection is ensured and promoted as an outlined product attribute.

In consequence, the results show valuable implication for theory and practice. The significantly high level of privacy in importance, which is even higher than price, indicates that SMD users demand more options to handle their user data and to protect their privacy. In contrary, customers of the two biggest app stores do not usually have the option of choosing between paying a monetary price or revealing their private user data. This imbalance provides a huge potential for innovating apps business models and its monetization. As for now, the user mostly has to decide if the apps provided utility is worth a privacy intrusion or not – meaning the user cannot use the app although a certain willingness-to-pay might exist. The study shows that at least offering apps in an alternative version with a monetary price and no usage of private user data could bear a great potential for success. Other options, such as permission management or administration of user data, could be another potential, but would represent a more restrictive way to deal with the privacy issue within SMD and apps. Since most of the apps requesting permissions regarding private user data do not function correctly without certain permissions, this approach might prove difficult to provide the full amount of utility of an app while containing only restricted permissions. Nevertheless, first developments to single permission management for each app in the Android OS are observable when taking a closer look at the newest OS 'Android 6.0 Marshmallow' [52].

5 Limitations and Future Research

Our paper deals with the question whether privacy is a crucial product attribute for users when buying apps. The results of the conducted CBC outline privacy as the product attribute ranking at the highest importance level and generating the highest utility value.

Due to the nature of our research, our study has some limitations. For example, in this paper we refer to the 'download' or purchase of apps. However, we are aware, that disclosing personal data is also related by app usage and deletion, which should be considered in future studies related to the topic. Furthermore, a particular app as a study object was required. Since the variety of apps could not be displayed with one app and the functionality has to be defined for the study object, the fictional CampusApp was selected. Our sample is not representative of all app users, as it includes a large group of university related participants. Based on the choice of the study object mostly students and employees of the addressed university were asked to answer the CBC. Although the focus on the four product attribute groups of price, privacy, ranking, and app-related was necessary due to the CBC complexity and justified by the low importance of vendor-related attributes in the pre-study, the results indicate that at least in the conscious priority ranking, vendor's reputation was considered quite important. Moreover, the preference structures' stability is questionable over time.

Starting with the high importance level of privacy within the purchase situation of apps, other privacy-sensitive areas, like private banking, insurance services, online social networks, or all kind of digital services linked with personal data could be investigated in more detail by using the CBC. This leads to the need of contemporarily and repeatedly conducted CBC in the future to maintain the topicality of the results and to validate privacy's standing as a crucial product attribute. Future CBC in the area of SMD and apps might include vendor-related attributes. Moreover, the elimination of choice sets could distort the results. Especially in the light of low effort situations and behavioral effects [25], taking a closer look at apps from various categories might offer interesting insights. Based on the social, political, legal, and additionally personal salience of privacy, further research in the area of privacy is essential. For example, the understanding and determination of the value term regarding privacy, the valuation of users' preference structures, or the explanation of the privacy paradox, offer a great deal of opportunities for future theoretical research and for a deeper understanding for more adequate attempts to assign a monetary value to privacy. Practically, research might focus on the options of permission management without losing functionality or the economical options of offering the same app in different versions regarding price and privacy. Additionally, those implications for apps, as well as SMD, and their relation towards privacy are also applicable to a very wide range of different research topics, e.g. investigation of the influence of privacy on different app types, as well as different demographical, social, or national groups.

Following the understanding of privacy as a crucial product attribute of apps, the legal regulation is called upon to preserve users of disclose their personal data in purchase situation they cannot control.

References

1. Weiser, M.: The computer for the 21st century. Scientific american 265, 94–104 (1991)
2. Yoo, Y.: Computing in everyday life: A call for research on experiential computing. MIS quarterly, 213–231 (2010)
3. Venkatesh, V., Thong, J.Y.L., Xu, X.: Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. MIS quarterly 36, 157–178 (2012)
4. Smith, H.J., Dinev, T., Xu, H.: Information Privacy Research: An Interdisciplinary Review. MIS quarterly 35, 989–1016 (2011)
5. Solove, D.J.: A taxonomy of privacy. University of Pennsylvania Law Review, 477–564 (2006)
6. Westin, A.F.: Social and political dimensions of privacy. Journal of social issues 59, 431–453 (2003)
7. Westin, A.F.: Privacy and Freedom, Atheneum. New York, 7 (1967)
8. Wellman, B.: The reconstruction of space and time: Mobile communication practices. Contemporary Sociology: A Journal of Reviews 39, 179–181 (2010)
9. Buck, C., Horbel, C., Kessler, T., Germelmann, C.C.: Mobile consumer apps: big data brother is watching you. Marketing Review St. Gallen 31, 26 (2014)
10. Clarke, R.: Internet privacy concerns confirm the case for intervention. Communications of the ACM 42, 60–67 (1999)
11. Chen, H.-T., Chen, W.: Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. Cyberpsychology, Behavior, and Social Networking 18, 13–19 (2015)
12. Dinev, T., Hart, P.: An extended privacy calculus model for e-commerce transactions. Information Systems Research 17, 61–80 (2006)
13. Acquisti, A., Brandimarte, L., Loewenstein, G.: Privacy and human behavior in the age of information. Science 347, 509–514 (2015)
14. Word Economic Forum: Personal Data: The Emergence of a New Asset Class, http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf
15. Spiekermann, S., Acquisti, A., Böhme, R., Hui, K.-L.: The challenges of personal data markets and privacy. Electron Markets 25, 161–167 (2015)
16. Bennett, C.J.: The political economy of privacy: a review of the literature. center for social and legal research, DOE genome project (Final draft), University of Victoria, Department of Political Science, Victoria (1995)
17. Berthold, S., Böhme, R.: Valuating Privacy with Option Pricing Theory. In: Economics of information security and privacy, pp. 187–209
18. Flender, C., Müller, G.: Type indeterminacy in privacy decisions: the privacy paradox revisited. In: Quantum Interaction, pp. 148–159. Springer (2012)
19. Buck, C., Germelmann, C.C., Eymann, T.: Datenweitergabe als Bedrohung? Konsumentenwahrnehmung am Beispiel mobiler Applikationen. In: Schmidt-Kessel, M., Langhanke, C. (eds.) Datenschutz als Verbraucherschutz, pp. 49–67. JWV Jenaer Wissenschaftliche Verlagsgesellschaft, Jena (2016)
20. Culnan, M.J., Armstrong, P.K.: Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization science 10, 104–115 (1999)
21. Malhotra, N.K., Kim, S.S., Agarwal, J.: Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. Information Systems Research 15, 336–355 (2004)

22. Xu, H., Teo, H.-H., Tan, Bernard C. Y., Agarwal, R.: The role of push-pull technology in privacy calculus: the case of location-based services. Journal of Management Information Systems 26, 135–174 (2009)
23. Pavlou, P.A., Gefen, D.: Building effective online marketplaces with institution-based trust. Information Systems Research 15, 37–59 (2004)
24. Norberg, P.A., Horne, D.R.: Privacy attitudes and privacy-related behavior. Psychology & Marketing 24, 829–847 (2007)
25. Dinev, T., McConnell, A.R., Smith, H.J.: Research Commentary: Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box. Information Systems Research 26, 639–655 (2015)
26. Schreiner, M., Hess, T.: On The Willingness To Pay For Privacy As A Freemium Model: First Empirical Evidence. In: ECIS 2013 (2013)
27. Chellappa, R.K., Sin, R.G.: Personalization versus privacy: An empirical examination of the online consumer's dilemma. Information Technology and Management 6, 181–202 (2005)
28. Wathieu, L., Friedman, A.A.: An Empirical Approach to Understanding Privacy Valuation. SSRN Journal (2007)
29. Spiekermann, S., Korunovska, J., Bauer, C.: Psychology of Ownership and Asset Defense. Why People Value Their Personal Information Beyond Privacy. SSRN Journal (2012)
30. Bauer, C., Korunovska, J., Spiekermann, S.: On the value of information - what facebook users are willing to pay. ECIS 2012 Proceedings (2012)
31. Krasnova, H., Eling, N., Abramova, O., Buxmann, P.: Dangers of 'Facebook Login' for Mobile Apps: Is There a Price Tag for Social Information? ECIS 2014 Proceedings (2014)
32. Hann, I.-H., Hui, K.-L., Lee, T., Png, I.: Online information privacy: Measuring the cost-benefit trade-off. ICIS 2002 Proceedings, 1–10 (2002)
33. Krasnova, H., Hildebrand, T., Guenther, O.: Investigating the value of privacy in online social networks: conjoint analysis (2009)
34. Pu, Y., Grossklags, J.: Using Conjoint Analysis to Investigate the Value of Interdependent Privacy in Social App Adoption Scenarios. ICIS 2015 proceedings (2015)
35. Böhler, H., Scigliano, D.: Traditionelle Conjointanalyse (in German). In: Baier, D., Brusch, M. (eds.) Conjointanalyse: Methoden, Anwendungen, Praxisbeispiele (in German), pp. 101–112. Springer, Berlin, Heidelberg (2009)
36. Baier, D., Brusch, M.: Erfassung von Kundenpräferenzen für Produkte und Dienstleistungen (in German). In: Baier, D., Brusch, M. (eds.) Conjointanalyse: Methoden, Anwendungen, Praxisbeispiele (in German), pp. 3–19. Springer, Berlin, Heidelberg (2009)
37. Balderjahn, I., Hedergott, D., Peyer, M.: Choice-Based Conjointanalyse (in German). In: Baier, D., Brusch, M. (eds.) Conjointanalyse: Methoden, Anwendungen, Praxisbeispiele (in German), pp. 129–146. Springer, Berlin, Heidelberg (2009)
38. Louviere, J.J., Woodworth, G.: Design and analysis of simulated consumer choice or allocation experiments: an approach based on aggregate data. Journal of marketing research, 350–367 (1983)
39. Cohen, S.H.: Perfect Union. CBCA marries the best of conjoint and discrete choice models. Marketing Research, 12–17 (1997)
40. Backhaus, K., Erichson, B., Weiber, R.: Fortgeschrittene Multivariante Analysemethoden (in German). Eine anwendungsorientierte Einführung, Berlin (2011)
41. Buck, C., Horbel, C., Germelmann, C.C., Eymann, T.: The Unconscious App Consumer: Discovering and Comparing the Information-Seeking Patterns among Mobile Application Consumers. ECIS 2014 Proceedings (2014)
42. Statista: Average prices for apps in the Apple App Store as of January 2016 (in U.S. dollars), http://www.statista.com/statistics/267346/average-apple-app-store-price-app/

43. Cowley, R., Suckley, M. and Jordan, J.: App Store Metrics, http://www.pocketgamer.biz/metrics/app-store/app-prices/
44. Statista: Schätzung des durchschnittlichen Preises kostenpflichtiger Apps für das iPhone und iPad weltweit in den Jahren 2009 bis 2022 (in US-Dollar), http://de.statista.com/statistik/daten/studie/170003/umfrage/preisentwicklung-von-apps-in-den-fuehrenden-app-stores-weltweit/
45. Buck, C.: App-privacy as an abstract value – Approaching contingency valuation for investigating the willingness to pay for app-privacy (2015)
46. Sunyaev, A., Dehling, T., Taylor, P.L., Mandl, K.D.: Availability and quality of mobile health app privacy policies. Journal of the American Medical Informatics Association (2014)
47. Statista: Mobile app monetization (2015)
48. Zhu, H., Xiong, H., Ge, Y., Chen, E.: Ranking fraud detection for mobile apps. In: He, Q., Iyengar, A., Nejdl, W., Pei, J., Rastogi, R. (eds.) the 22nd ACM international conference, pp. 619–628 (2013)
49. Sawtooth Software Inc.: The CBC System for Choice-Based Conjoint Analysis. Version 8
50. Johnson, J., Huber, J., Orme, B.: A Second Test of Adaptive Choice Based Conjoint Analysis. (The Surprising Robustness of Standard CBC Designs). In: Sawtooth Software Inc. (ed.) Proceedings of the Sawtooth Software Conference on Perceptual Mapping, Conjoint Analysis and Computer Interviewing, pp. 219–236 (2004)
51. Gensler, S.: Ermittlung von Präferenzen für Produkteigenschaften mit Hilfe der Choice-Based Conjoint Analyse, Teil II. Frankfurt am Main (2006)
52. Google Inc.: Android 6.0 Marshmallow, https://www.android.com/intl/de_de/versions/marshmallow-6-0/