Association for Information Systems

AIS Electronic Library (AISeL)

ICEB 2015 Proceedings

International Conference on Electronic Business (ICEB)

Winter 12-6-2015

App-Privacy As An Abstract Value – Approaching Contingent Valuation For Investigating The Willingness To Pay For App Privacy

Christoph Buck

APP-PRIVACY AS AN ABSTRACT VALUE – APPROACHING CONTINGENT VALUATION FOR INVESTIGATING THE WILLINGNESS TO PAY FOR APP PRIVACY

Christoph Buck, University of Bayreuth, Germany, Christoph.buck@uni-bayreuth.de

ABSTRACT

Apps can be seen as the embodiment of ubiquitous computing, i.e. the creation of environments saturated with computing and communication capability, integrated with human users. App markets are typical examples of so-called free or freemium markets, i.e. most apps include (at least) a free basic version. However, this does not mean that consumers do not have to pay for the benefits they derive. More precisely, private information of consumers is generated as the majority of apps receives, stores, or processes personal data, although sometimes other revenue mechanisms are used simultaneously. Given the fact that consumers' information privacy as personal data privacy is a major part of the economic exchange when downloading and using apps, app privacy is determined as an attribute of the value proposition of apps. The current paper approaches the contingent valuation for measuring the willingness to pay for app privacy as an abstract value.

Keywords: Privacy, Security, Willingness to Pay, Contingent Valuation.

INTRODUCTION

Let's face reality – privacy concerns are ubiquitous, just like smart mobile devices (SMDs) and the vast amount of user data they create. Recent developments in computing and the seemingly endless possibilities of collecting, connecting, processing, and distributing data, sometimes even without the actual knowledge of users, lead to huge amounts of user data [40].

With the disruptive innovations of the iPhone and the iPad, leading to the product class of smart mobile devices (SMDs), software in the form of mobile applications (apps) diffused in the everyday life of consumers. 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 [51]. 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" [53, p. 213].

Apps in combination with SMDs can be regarded as today's archetype of ubiquitous computing. At the same time, this development has considerably contributed to the emergence of a new user type. These new users integrate apps into their everyday lives, which leads to fundamental changes concerning how users interact with computing devices and systems [46]. SMDs provide plenty of sensors and technical features. Combined with ever-increasing processing power, storage capacity, communication bandwidth, and ever-present WiFi access, mobile technology made the vision of ubiquitous computing come true. The combination of tangible computing, the digitalization of everyday artifacts, and the global infrastructure already became milestones of the integration of apps into everyday life. Thus, apps use the broad opportunities given by integrated sensors, connect several kinds of data, enable new value propositions and provide effective digital solutions for needs previously addressed in a non-digital way.

Apps can be used to perform every kind of task and users benefit, while handling their everyday routine. Everyday activities, e.g., comprising navigation, buying lists, communication, scheduling, gaming, information, sports, and learning, are almost 'naturally' carried out or supported through the use of apps, or as Apple puts it in one of their slogans: "There is an app for that" [1].

App markets are typical examples of so-called free or freemium markets, i.e. most apps include (at least) a free basic version [34]. However, this does not mean that consumers do not have to pay for the benefits they obtain. Although there is often no money involved when purchasing an app, the provider does not offer the app 'for free'. More precisely, consumers' private information are taken as 'currency', as the majority of apps receives, stores, or processes personal data, although sometimes other revenue mechanisms are used simultaneously (e.g. in-app advertising, monetary payment for the app). Nonetheless, consumers can still benefit from 'free apps' in exchange for their personal data. Hence, personal data and privacy can be regarded as the predominant 'currency' in app markets.

As a reaction to the recent developments in computing and the seemingly endless possibilities of collecting, connecting, processing and distributing, [40] [5], consumers have developed growing privacy concerns. They primarily want to know who is able to access their data, but they are also worried by the general use and sale of it. Consumers' concerns about privacy lead to an increasing demand for information and a movement for privacy [23] [38]. Although user data might be stolen or used illegally, using it in a legal or permissible way is more common and wide spread [28].

Given the fact that consumers' information privacy is a major part of the economic exchange, when downloading and using apps, app privacy, and the corresponding settings, have to be determined as an attribute of the value proposition of apps. In order to

understand consumers' concerns and clearly define the necessity of user data protection, it is crucial to quantify the value of privacy for consumers, using the concept of willingness-to-pay. Therefore, the paper will address the following research question:

1. Do consumers have a willingness to pay for app privacy?

To answer these research questions, the remainder of this article is structured as follows. In the following section, I will define privacy as a product attribute of apps. Further, I will introduce the underlying terminology of privacy into the digital age and the value of privacy in the context of apps. Following this, I will describe the methodology of the contingent valuation of app privacy and will present the key findings of the study. Finally, I will address some limitations and conclude with suggestions for further research.

DIGITAL PRIVACY AS PRODUCT ATTRIBUTE

Privacy in the Digital Age

Since privacy is addressed to so many fields of social sciences and different definitions are used in different areas of everyday life, it is known as an „umbrella term" [42]. Thus, the term 'privacy' lacks of a holistic definition, due to the different perspectives of varying disciplines [40] [42] [4]. Research in specific areas needs to be more precise about the particular area privacy is focusing on [40] [42]. It is widely agreed on, that privacy "is in disarray and nobody can articulate what it means" [42, p. 477].

First of all, physical and informational privacy have to be distinguished. Physical privacy relates to the "access of an individual and/or the individual's surroundings and private space" [40, p. 990]. Contrary, informational privacy only refers to information that is individually identifiable or describes the private informational spheres of an individual. Although informational privacy is rooted in the fundamental concept of physical privacy, both are subsumed under the term of "general privacy" [40]. Since this article deals exclusively with informational privacy, I am going to use privacy as a reference for informational privacy. A distinction will be made by stating physical or general privacy, if necessary.

The development of general privacy and in particular of informational privacy, is highly correlated with the evolution of information technology [26] [29] [32] [40]. [50] explains the evolution of privacy in a chronological way consisting of four stages. In the first stage, which ended in 1961, privacy was a social issue of low concern. Similar to the limited developments in information technology [40], privacy was "interesting but neither primary nor even secondary in social and political salience" [50, q. 8]. In the second stage, advocacy journalism and television-age media competition gained more and more importance and started to warn the public audience about privacy breaches, raising the first informational privacy concerns. As a result, the first detailed national survey was conducted in the United States in 1978, showing that already 76% of the subjects believed that "privacy should be added to the rights of life, liberty, and the pursuit of happiness" [50, p. 12], which constitute the most fundamental privileges of the American society. Overall, privacy gained in importance on a social, political, and legal level and lead to the very first generation of privacy acts and laws [50]. The third stage in the 1980s was triggered and accompanied by the technological development of computing and network systems. However, the collection and usage of personal information "did not break new ground" [50, p. 10]. Processing information became cheaper, faster, and more efficient. But since computers were not connected to each other, information remained in separate data bases [50]. Although several federal legislative and governmental activities took place at that point, information privacy remained on the second level of social and political salience. The rise of the Internet, combined with the development of Web 2.0, and particularly the terrorist attacks of 9/11/2011 in the United States, lead to a revolution in privacy issues. Informational privacy became a tier-one social and political topic [40] [50]. Additionally, increasing worldwide communication, trade, travel, and marketing activities resulted in the development of globalization and simultaneous informational collection, as well as in concerns regarding these practices [50]. Back in 1985, computer scientists like Larry Hunter did not expect new developments in gathering, but in analyzing willingly shared information [32]. To implement these developments this article proposes to add a fifth stage to [50] definitional approach, regarding the evolution of the information privacy concept: The fourth Era of Privacy Development (2003-present).

In the 21st century, SMDs conquered the market of consumer electronics. Equipped with sophisticated sensors and advanced computer hardware and software, they entail wide-reaching new ways of collecting and connecting user data [36]. As the "pocket knife of communication" [48], SMDs possess a vast amount of connected sensors, devices, and functions. Throughout these functions, the possibilities of gathering information are virtually endless. Future prospects in relation to these applications promise even more opportunities to expand data collection and immediate analysis of data.

To evaluate privacy as an attribute of apps, it is important to provide a definition and conceptual framework of app privacy. While [12] defines privacy "as a moral right or a legal right", many researchers suggests privacy as one's ability to control information about oneself [4]. Researchers in various disciplines stressed control as the key dimension of privacy [40] [4] [22] [30] [33] [37] [41] [44]. The concept of privacy as a legal right in the modern sense, can be traced back to [47], who said the nucleus of privacy is "the right to be let alone." The vast diffusion of network SMDs via the Internet and the broad access of consumer software, facilitate the development of an active approach to protecting privacy due to SMDs and apps tracking, storing and aggregating personal data without being recognized [11]. Furthermore, privacy means taking control over information about consumers' lives which is why consumers should be empowered to protect themselves instead of simply allowing them to be passively left alone

[20]. According to [49] privacy is defined as"… the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Consequently, privacy is the ability to control the acquisition and use of one's personal information [49]. The concept of autonomous and self-determined control over the disclosure of private information is closely related to information and communication technologies and thereby to SMDs and apps [14].

In app markets consumers are able to control their privacy disclosure during the purchase process. Before downloading an app, they have to accept the privacy settings, as part of economic exchange. Thus, consumers can actively control their disclosure of personal data and third parties' intervention into their privacy. Consequently, consumers have greater responsibility than they had before, using SMDs to decide to which extent they would like to share their personal information in the moment of downloading an app [11].

Privacy in the Context of Apps

The advancements of SMDs, Web 4.0, the Internet of Things (IoT), and other technical revolutions continued to raise more and more concerns about informational privacy [3]. Through these "unprecedented possibilities to collect, store, aggregate and analyze user data" [26, p. 1] via SMDs and apps, privacy concerns remained on the highest tier of public interest. Apps, like traditional software, can be characterized as closed and not integrated software packages, which depend on their underlying operating system (OS) [17]. Apps are "application software programs, which use web and cloud applications and run on SMDs. They can be purchased and installed, depending on their operating system and perform (highly fragmented) everyday tasks. Importantly, apps are embedded in mobile ecosystems, i.e. OS-based platforms, which provide profile-bound ubiquitous services for mobile devices" [7, p. 3].

Regarding data quality, recent developments in mobile technology and an ever increasing digitalization 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. Apps are embedded in a unique architecture, which allows for an aggregation of fragmented pieces of personal data, gained from SMDs and apps, and can be classified in a four-tier model [7].

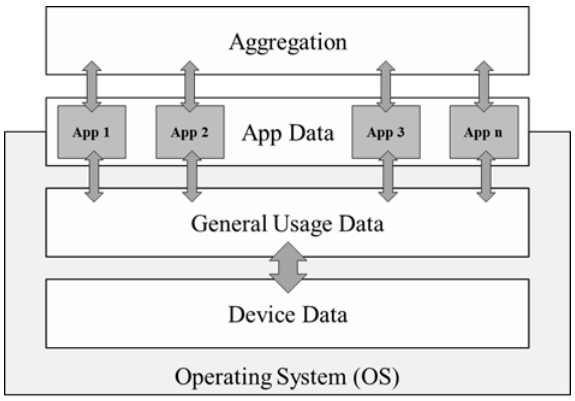

Figure 1. Four-Tier Model of App Data Aggregation

The first tier includes basic consumer data, which is required for the enrollment and already generates first-class information to personalize the user profile, for example verified e-mail address, phone numbers, IMEI, UDID and, when using the app store, payment information like credit card and banking information [19]. The second tier represents the ecosystem's ability to track and store all data generated when using the basic OS. The use of this data can be extended to a moving profile or a far-reaching profile of consumers' social environment. The third tier refers to the ability of a third party vendor to use specific data of consumers' app usage. Apps perform everyday tasks; therefore app usage data gives wide-reaching insights into consumers' everyday lives. In addition, the information can be recorded and personalized by the third party vendor by downlinking it to the OS, and thereby allowing for fundamental insights into consumers' behavior [18]. Finally, a comprehensive user profile is generated by fourth party aggregators like Google or Flurry, representing the fourth tier. These aggregators gather information from thousands of app vendors and can create a holistic profile of users' lives. Personal information collected via apps are in a digital format and can be copied, transmitted, and integrated, which enables third parties to construct thorough descriptions of individuals and cause a serious threat to privacy if these information are not handled properly [28].

The mere technical characteristics of apps show the range of privacy issues which are involved when using apps. Because of the everyday life integration, apps address all four privacy dimensions identified by [12]: privacy of a person, personal behavior privacy, personal communication privacy, and personal data privacy. When addressing apps, the most important dimension is the personal data privacy, which directly affects the other three dimensions. Via apps and the mobile internet, real time and real life data can be collected, aggregated, and analyzed faster, in larger volume, and at a greater personal life depth than ever [28]. [12] privacy dimensions cover a very broad field and have to be extended by the classification of information privacy of [41], which

can be subsumed under [12] dimensions of privacy of a person. [41] have identified four dimensions of information privacy as personal data privacy: collection, unauthorized secondary use, improper access, and errors dissemination, and invasion. First of all the collection of personal data via apps is multilayered and not transparent for consumers. When downloading an app, consumers have to agree to data permission of providers whose actions and consequences they cannot evaluate. Furthermore, data can be collected without individuals being actually aware of it [5]. The unauthorized second use of data is something consumers often cannot understand and control, moreover often they are not aware of the amount of data being collected. Additionally, the usage refers to data for other purposes than those for which they were originally collected.

Subsequently, the purchase and usage of apps involves privacy risks at a high degree and regarding all dimensions of privacy for consumers. Even though privacy has developed and changed drastically over the last several decades, [49] [50]'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" [49, p. 3]. Combining the development of technology, as the influence on informational privacy, and [49] [50]'s definition, it is to scrutinize whether the individuals of the 21st century, with the omnipresent computing of SMDs, are still able to determine what personal information is accessible to others. To pursue this question I will take an in-depth look at the definitional approaches on informational privacy, as well as distinguish privacy from similar and often misinterpreted concepts.

Consequently, in this paper privacy is defined as the ability to control the acquisition and use of one's personal information [49]. The concept of autonomous and self-determined control over the disclosure of private information is closely related to information and communication technologies and therewith to SMDs and apps [14]. In app markets consumers are able to control their privacy disclosure during the purchasing process. Thus, consumers can actively control their disclosure of personal data and the grasping of privacy from third parties [11]. The current paper exhibits app consumption (for this purpose predefined as the downloading decision) as a highly privacy related behavior, as it covers all four privacy dimensions identified by [12]: personal data privacy, personal communication privacy, personal behavior privacy, and privacy of a person. Via apps and the mobile internet, real time and real life data can be collected, aggregated, and analyzed faster, in larger volume, and at a greater personal life depth than ever [28]. According to [41] consumers' information privacy as personal data privacy, in the context of the purchase situation, is affected via apps and the mobile internet in terms of collection, unauthorized secondary use, and improper access.

App Privacy as an Abstract Value

[15, p. 61] stated that privacy "is a highly cherished value, few would argue that absolute privacy is unattainable." While this describes consumers' perspective, the personal information and highly personalized data collected via apps have a huge economic value. Due to this, users are supposed to undertake an anticipatory, rational weighting of risks and benefits when confronted with the decision to disclose personal information or conduct transactions [28] [52].

This perspective leads [6] to bring up the idea of privacy as a commodity. 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 [40]. An example for this shift from privacy as a right, to an economically exchangeable commodity is summarized under the term of "self-surveillance" [40]: Individuals cooperate in the information gathering process, forfeiting some of their privacy in exchange for a particular benefit [25]. Nevertheless, it remains unclear if this is a simple bargain process or if the current privacy crisis is the result of a market failure by the technological development or existing privacy legislation [21] [27]. [13] introduced this privacy trade-off as the privacy calculus, which has been extensively studied in several contexts, such as e-commerce [15], the Internet [28] [16] or mobile applications [52]. The privacy calculus assumes a correct understanding of the monetary value of privacy and therewith a tangible willingness to pay for privacy of the consumers. Most privacy measurement instruments are supposed to be too general to reflect the true essence of privacy-related anxiety [39]. Also there is a fundamental gap between how users claim to feel about privacy and how they act in real-life settings [43] [2].

Regarding the pricing of information privacy, the value-based definitional approach towards information privacy, along with its commodity concept, offers the best match with the theory of willingness-to-pay. This is particularly evident in the observation of the phenomenon of the privacy calculus, which was validated by several studies: Consumers consciously calculated cost-benefit trade-offs based on the perceived risks and benefits of an informational disclosure. Both the concepts of maximization and reservation price are based on the perceived value of a product and therefore generally applicable and consistent with the value-based definitional approach of information privacy. The maximization price is based on the consumer's reference value, arising from the price of an alternative good or service. However, it is not possible to calculate a reference value for information privacy, as there are no alternatives to this particular good or service. Therefore, using the concept of a maximization price to determine a consumer's willingness-to-pay for privacy is not applicable. On the other hand, the reservation price does not need any reference values of alternative goods or services. It is based on the consumer's utility or at least at the perceived value a product or service offers. In order to quantify the willingness-to-pay for privacy it is necessary to determine the monetary equivalent, which is based on the consumer's perceived value. This perceived value individually differs to a large extent due to the simple fact that information privacy is valued subjectively and that the value of certain information types is too abstract to be described successfully. As they also suffering from the privacy paradox, studies and surveys about individuals' utility functions of

information privacy were not able to determine such a value after all. Following this, this article defines privacy as an abstract value.

In the end, information privacy is evaluated subjectively by every individual and the value of different information types is abstract and intangible. Taking a closer look at this particular situation, similarities with the paradigm shift from goods- to service-dominant logic in marketing can be detected [45]. As [45] point out, the orientation and the academic focus shifted from tangibles toward intangibles, such as skills, information, and knowledge. While the process of exchanging becomes more important, interactivity, connectivity, and ongoing relationships are also gaining importance. The authors suggest that the "static and discrete tangible good" [45] is no longer the appropriate unit of exchange. Additionally, they argue for operant resources to become the next unit of exchange. They are intangible, continuous, and dynamic and stand for the application of competences, specialized human knowledge, and skills [45]. Applied to the area of information privacy, the service-dominant logic offers a new and more accurate view on what type of product, service or information is traded. It offers a new perspective on the co-creation of information-gathering companies and the users which provide knowledge and skills in form of their user data.

METHODOLOGY

Survey Design

Based on the classification of app privacy as an abstract value, a contingent valuation (CV) via an online survey was conducted. Due to the fact that transparent and trustable market prices are not available for privacy and personal data contingent valuation is chosen as a qualified instrument to measure the willingness to pay for privacy [9]. Moreover, the loss of privacy is a very subjective procedure which cannot be objectified. To depict a holistic estimation of the abstract value of app privacy of consumers, this methodology was applied because of CVs ability to quantify abstract values. Compared to common approaches of measuring preferences, it is not limited in measuring the utility value based on the observable behavior in related markets [10].

Based on a narrative scenario, participants were asked to appraise their willingness to pay (WTP) for high privacy settings [8]. According to the control-based definition of app privacy and the dimensions of collection, unauthorized secondary use, and improper access, consumers could estimate their WTP for avoiding these risks. In the first place this was implemented by offering a bidding game according to generic app prices to cover the so-called software protection. In the second place participants were asked to mention their WTP for hardware protection through a privacy dongle. Figure 2 illustrates the sequences of the conducted online survey.

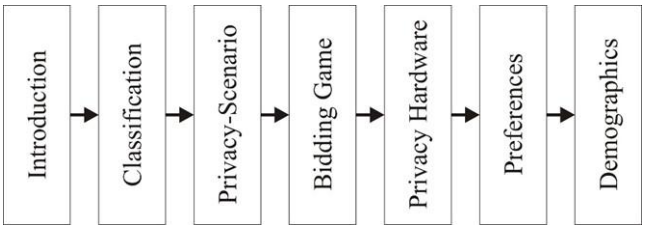

Figure 2. Setup of the Study

After a short introduction in section one of the survey the participants were asked in section two if they have a SMD and if they have ever downloaded an app (filter questions). If participants had no SMD or did never download an app they were excluded from the survey. It must be assumed that experience in the field of app downloading is crucial for valid responses [35]. Following the filter questions participants had to state which apps they have downloaded by means of a list about the 20 most common used apps in Germany.

Departing from classic CV, two different privacy scenarios were designed in the third section. The first narrative scenario was based on the tagesschau app, the app of the federal German news channel. This app is supposed be recognized as a trustworthy app also because of the correspondent federal German news channel. The second narrative scenario was conducted with the instant messaging app whatsapp which can be defined as a non trustworthy app in the consequence of public news about whatsapps privacy breaches in 2014. Both scenarios were randomly distributed to the participants. Additionally, questions regarding the manufacturer of the used SMDs were asked to classify the participants depending on the underlying ecosystem provider.

The fourth section represents the core of the contingent valuation study. Because of the simplicity of the analysis and convenience of the participants randomly closed-ended questions were used in the survey. The participants were supposed to answer the question about their willingness to pay for a privacy markup of (randomly) 0,49€, 1,99€ or 5,99€ with a dichotomous choice (yes/no). To improve evidence a bidding-game followed to iteratively test consumers' willingness to pay for privacy markups [24] [31]. Figure 3 illustrates the structure of the bidding game.

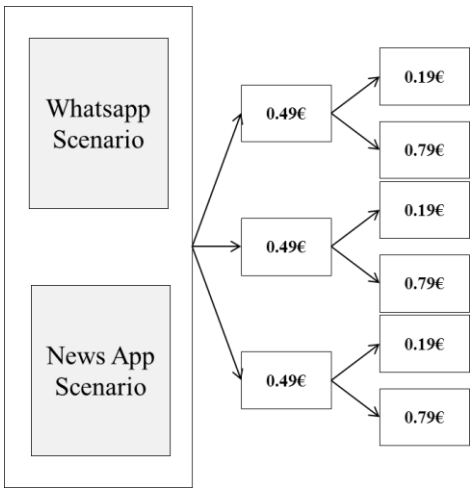

Figure 3. Structure of the Bidding Game

In the fifth section participants were asked about their willingness to pay for privacy enhancing hardware and software upgrades. After stating their preferences in section six, demographics were prompted in section seven.

Data Collection and Results

All items regarding consumers' willingness to pay for privacy were measured on dichotomous scales ranging from "yes" (1) to "no" (2) and pending questions. Data collection took place between June 2014 and October 2014 in Germany. Consumers were invited to participate in an online survey via social media (Facebook, Xing, etc.), (university) mailing lists, and postings on the website of a regional sports club. Altogether, 1171 participants subscribed to the study. 998 participants (85,2%) who use an SMD as well as downloaded at least one app (filter questions) completed the contingent valuation part of the survey and were included in the subsequent data analysis.

Of the remaining individuals, 38.8% (N = 387) were female and 61.2% were male (N = 611). Most of the respondents were younger than 50 years (91.2%; N = 907). The largest group were Teenagers between 13 and 19 years of age (33.5%; N = 334), followed by participants who were younger than 13 years old (25.4%; N=253) and participants between 20 and 29 years of age (33.5%; N = 240). The mean value of the participants age was 20.04 (SD=10.98). Regarding the level of school education it is noticeable that 96.89% have an A-Level/Highschool Certificate (75.55%) or a secondary school level certificate (21.34%). Respondents' OS-affiliation was identified according to the device manufacturer. 524 participants (52.51%) used iOS and 474 (47.49%) used non-iOS.

Table 1. Descriptive Statistics

Gender	Count	Percentage
Female	387	38,78%
Male	611	61,22%
Total	998	100,00%

Age	Count	Percentage
younger than 13	253	25,50%
13 to 19 (Teenager)	334	33,67%
20 to 29	240	24,19%
30 to 39	89	8,97%
40 to 49	60	6,05%
50 to 59	11	1,11%
60 and older	5	0,50%
no response	6	0,60%
Total	998	100,60%

School Education	Count	Percentage
no degree	22	2,20%
Secondary school leaving certificate	213	21,34%
A level/ High-school certificate	754	75,55%
no response	9	0,90%
Total	998	100,00%

Operating System Affiliation	Count	Percentage
iOS	524	52,51%
non-iOS	474	47,49%
Total	998	100,00%

Number of downloaded Apps	Count	Percentage
1 to 10	188	18,84%
11 to 20	283	28,36%
21 to 30	190	19,04%
31 to 40	102	10,22%
41 to 50	67	6,71%
51 to 60	33	3,31%
61 to 70	21	2,10%
71 to 80	30	3,01%
81 to 90	16	1,60%
more than 90	49	4,91%
no response	19	1,90%
Total	998	100,00%

App Experience in months	Count	Percentage
up to 11	120	12,02%
12 to 23	197	19,74%
24 to 35	263	26,35%
36 to 47	198	19,84%
48 to 50	106	10,62%
60 to 71	46	4,61%
more than 71	51	5,11%
no response	17	1,70%
Total	998	100,00%

Downloads of narrative scenario apps	Count	Percentage
Whatsapp downloaded	906	90,78%
Whatsapp not downloaded	92	9,22%
Total	998	100,00%
News App downloaded	282	28,26%
News App not downloaded	716	71,74%
Total	998	100,00%

Concerning the experience variables the data set is structured as following: the participants have downloaded about 30 apps on average (mean value=30.6; SD=24.46). Most people have downloaded 11 to 20 apps in their usage history (28.36%), followed by 21 to 30 apps (19.04%), and 1 to 10 apps (18.84%). The vast majority of the participants had up to 35 month of app experience (88.58%). The largest group were participants with 24 to 35 months of app experience.

Regarding the narrative privacy scenarios the availability of the chosen scenario apps is important. With 90.78% the vast majority of the participants had the instant messaging app whatsapp on their device. The supposed trustworthy app of the German federal news channel (tagesschau) was downloaded by only 28.26% of all participants. For further analyses this seems not to be critical under the assumption that the news channel is well known by all participants as a trustworthy institution.

Table 1 provides an overview regarding the descriptive statistics and the distribution of the participants regarding different classification criteria.

The analysis of the bidding game for the news app produced the following results. The vast majority of the participants had in the first round of the bidding game the willingness to pay for privacy in the 0.49€ game (82.50%) and in the 1.99€ game (78.13). When it comes to pay 5.99€ for a privacy markup 47.83% had the willingness to pay for it. Figure 4 illustrates the detailed results of the bidding game regarding a privacy markup in terms of the trustworthy news app.

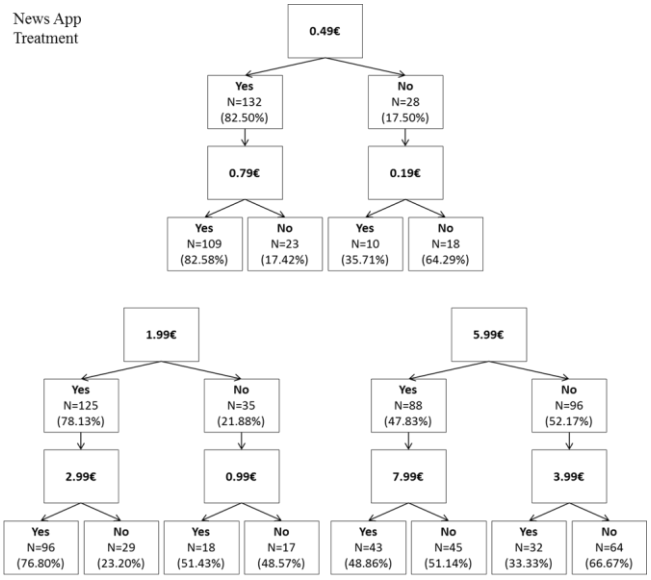

Figure 4. Bidding Game for News App

In comparison, the analysis of the bidding game for the instant messaging app produced the following results. The vast majority of the participants had in the first round of the bidding game the willingness to pay for privacy in all three game settings. In the 0.49€ game 94.41% had the willingness to pay for the privacy markup followed by 90.06% in the 1.99€ game and 74.42% in the 5.99€ game. Compared with the news app treatment all three games settings had a much higher willingness to pay for the privacy markup. Furthermore, the results from the second round of the bidding games show higher willingness to pay for app privacy in all compared settings.

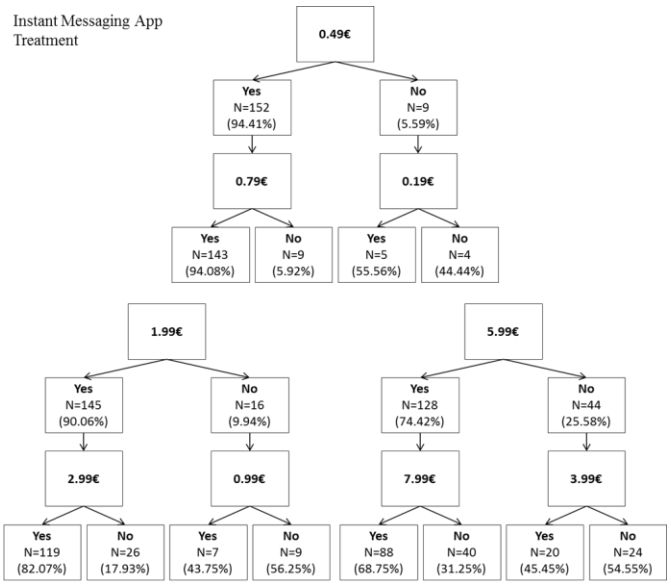

Figure 5. Bidding Game for Instant Messaging App

Using cross tabulation the differences in the answers of participants regarding their willingness to pay for privacy markups in the two conditions of an uncritical and a critical app were compared. The results of the analysis show significant differences ($X^2_{game\ 0.49}=0.001$; $X^2_{game\ 1.99}=0.003$; $X^2_{game\ 5.99}<0.001$) for the two conditions in terms of their initial willingness to pay for privacy markups (round 1). Thus, in case of being confronted with a critical app consumers have a significantly higher willingness to pay for privacy markups then when the perceived insecurity of the app is rather low.

Furthermore, the results demonstrate that in the case of a rather low price (0.49€) for a privacy markup and in the case of a rather high price (5.99€) consumers' willingness to pay even more than the initial price was significantly higher ($X^2_{game\ 0.49}=0.002$; $X^2_{game\ 5.99}<0.003$) in the critical app condition than in the non-critical app condition. However, no differences between the participants in the two conditions were observed regarding their willingness to pay a lower price than the initially offered price for a privacy markup.

LIMITATIONS

The paper deals with the question whether consumers have the willingness to pay for a privacy markup in a given app privacy settings. The results of the conducted contingent valuation show that most consumers do have the willingness to pay for a privacy markup. Due to the nature of the research in the field of contingent valuation, the study has some limitations. For example, while in this paper I refer to the 'consumption' of apps, it must be recognized that I limited my considerations to 'purchasing' apps. However, I am aware, that consuming apps also includes app usage and deletion, which should be considered in future studies related to the topic. The chosen sample is not representative of all app consumers, as it includes a large group of students and younger people. The predefined starting points of the bidding game settings of 0.49€, 1.99€ and 5.99€ are generic not validated by results of earlier research.

CONCLUSION AND FUTURE RESEARCH

With the download of an app, consumers potentially give away their personal data without knowing what the publisher or the OS provider is using it for. Although a considerable amount of information on the use of consumers' data is provided within the app stores, it is questionable if consumers use and evaluate the information in a suitable manner. The minimized information consumption and its misinterpretation are caused by the distorted perception of apps and therewith by the distorted risk perception. Nevertheless, the download and usage of apps are characterized by a typical situation of economic exchange: according to the view of privacy as commodity consumers pay a vast number of apps with their disclosed personal data. The presented paper defines privacy as an abstract value which is difficult for consumers to evaluate. With the approach of the contingent valuation the paper provides a first step in validation consumers' willingness to pay for privacy.

Nevertheless, because of the increasing importance of personal information and increased security breaches in a more and more interconnected and digitized world privacy and its evaluation further research on privacy is necessary.

REFERENCES

[1] Apple Inc. (2015) 'Apple trademark list', Apple Inc., available at https://www.apple.com/legal/intellectual-property/trademark/appletmlist.html (accessed 25 October 2015).

[2] Acquisti, A. & Gross, R. (2006) 'Imagined communities: Awareness, information sharing, and privacy on the Facebook', *Privacy enhancing technologies*, pp. 36-58.

[3] Bélanger, F. & Crossler, R. E. (2011) 'Privacy in the digital age: a review of information privacy research in information systems', *MIS quarterly*, Vol. 35, No. 4, pp. 1017-1042.

[4] Bélanger, F., Hiller, J. S. & Smith, W. J. (2002) 'Trustworthiness in electronic commerce: The role of privacy, security, and site attributes', *The Journal of Strategic Information Systems*, Vol. 11, No. 3, pp. 245-270.

[5] Bélanger, F. & Hiller, J. S. (2006) 'A framework for e-government: privacy implications', *Business process management journal*, Vol. 12, No. 1, pp. 48-60.

[6] Bennett, C. J. (1995) '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,

[7] Buck C., Horbel C., Germelmann C.C. & Eymann T. (2014) 'The unconscious app consumer: Discovering and comparing the information seeking patterns among mobile application consumers', *ECIS 2014 Proceedings*, pp. 1–14.

[8] Carson, R. T. (2000) 'Contingent valuation: a user's guide', *Environmental science & technology*, Vol. 34, No. 8, pp. 1413-1418.

[9] Carson, R. T. (2012) 'Contingent valuation: A practical alternative when prices aren't available', *The Journal of Economic Perspectives*, Vol. 26, No. 4, pp. 27-42.

[10] Carson, R. T., Flores, N. E. & Meade, N. F. (2001) 'Contingent valuation: Controversies and evidence', *Environmental and resource economics*, Vol. 19, No. 2, pp. 173-210.

[11] Chen, H.-T. & Chen, W. (2015) 'Couldn´t or wouldn´t? The influence of privacy concerns and self-efficacy in privacy management on privacy protection', *Cyberpsychology, Behaviour, and Social Networking*, Vol. 18, No. 1, pp. 13-19.

[12] Clarke, R. (1999) 'Internet privacy concerns confirm the case for intervention', *Communications of the ACM*, Vol. 42, No. 2, pp. 60-67.

[13] Culnan, M. J. & Armstrong, P. K. (1999) 'Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation', *Organization science*, Vol. 10, No. 1, pp. 104-115.
[14] Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I. & Colautti, C. (2006) 'Privacy calculus model in e-commerce–a study of Italy and the United States', *European Journal of Information Systems*, Vol. 15, No. 4, pp. 389–402.
[15] Dinev, T. & Hart, P. (2006) 'An extended privacy calculus model for e-commerce transactions', *Information Systems Research*, Vol. 17, No. 1, pp. 61-80.
[16] Dinev, T., Xu, H., Smith, J. H. & Hart, P. (2013) 'Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts', *European Journal of Information Systems*, Vol. 22, No. 3, pp. 295-316.
[17] Egele, M., Kruegely, C., Kirda, E. & Vigna, G. (2011) 'PiOS: Detecting privacy leaks in iOS applications', available at http://www.cs.ucsb.edu/~chris/research/doc/ndss11_pios.pdf (accessed 25 October 2015).
[18] Enck, W. (2011) 'Defending users against smartphone apps: Techniques and future directions', In Hutchison, D. et al. (eds.), *Information Systems Security, Lecture Notes in Computer Science*, 7093, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 49–70.
[19] Felt, A.P., Finifter, M., Chin, E., Hanna, S. & Wagner, D. (2011) 'Asurvey of mobile malware in the wild', In: Jiang, X. (eds.) *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, Chicago, Illinois, USA, pp. 3-14.
[20] Fried, C. (1968) 'Value of life', *The. Harv. L. Rev*., Vol. 82, p. 1415.
[21] Garfinkel, S. (2000) 'Database nation: The death of privacy in the 21st century', O'Reilly Media.
[22] Goodwin, C. (1991) 'Privacy: Recognition of a consumer right', *Journal of Public Policy & Marketing*, pp. 149-166.
[23] Groopman, J. & Etlinger, S. (2015) 'Consumer perceptions of the privacy in the internet of things: What brands can learn from a Concerned Citizenry', available at http://www.altimetergroup.com/pdf/reports/Consumer-Perceptions-Privacy- IoT-Altimeter-Group.pdf (accessed 25 October 2015).
[24] Hoyos, D. & Mariel, P. (2010) 'Contingent valuation: Past, present and future', *Prague economic papers*, Vol. 4, pp. 329-343.
[25] Klopfer, P. H. & Rubenstein, D. I. (1977) 'The concept privacy and its biological basis', *Journal of social issues*, Vol. 33, No. 3, pp. 52-65.
[26] Krasnova, H. & Kift, P. (2012) 'Online privacy concerns and legal assurance: A user perspective', Teoksessa AIS SIGSEC WISP Workshop on Information Security and Privacy.
[27] Laudon, K. C. (1996) 'Markets and privacy', *Communications of the ACM*, Vol. 39, No. 9, pp. 92-104.
[28] Malhotra, N. K., Kim, S. S. & Agarwal, J. (2004) 'Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model', *Information Systems Research*, Vol. 15, No. 4, pp. 336-355.
[29] Marx, G. T. (2001) 'Murky conceptual waters: The public and the private', *Ethics and Information technology*, Vol. 3, No. 3, pp. 157-169.
[30] Milne, G. R. & Rohm, A. J. (2000) 'Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives', *Journal of Public Policy & Marketing*, Vol. 19, No. 2, pp. 238-249.
[31] Niklitschek, M. & León, J. (1996) 'Combining intended demand and yes/no responses in the estimation of contingent valuation models', *Journal of Environmental Economics and Management*, Vol. 31, No. 3, pp. 387-402.
[32] Nissenbaum, H. (1998) 'Protecting privacy in an information age: The problem of privacy in public', *Law and philosophy*, Vol. 17, No. 5, pp. 559-596.
[33] Nowak, G. J. & Phelps, J. (1997) 'Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters', *Journal of Interactive Marketing*, Vol. 11, No. 4, pp. 94-108.
[34] Osterwalder, A. & Pigneur, Y. (2010) 'Business model generation: A handbook for visionaries, game changers, and challengers', John Wiley & Sons.
[35] Payne, J. W., Bettman, J. R., Schkade, D. A., Schwarz, N. & Gregory, R. (2000) 'Measuring constructed preferences: Towards a building code', *In Elicitation of preferences*, pp. 243-275.
[36] Pejovic, V. & Musolesi, M. (2015) 'Anticipatory mobile computing: Asurvey of the state of the art and research challenges', *ACM Computing Surveys (CSUR)*, Vol. 47, No. 3, p. 47.
[37] Schwartz, P. M. (2000) 'Beyond Lessig's code for internet privacy: Cyberspace filters, privacy control, and fair information practices', *Wis. L. Rev.*, p. 743.
[38] Shah, R. (2015) 'Do privacy concerns really change with the internet of things?', available at http://www.forbes.com/sites/rawnshah/2015/07/02/do-privacy-concerns-really-change-with-the-internet-of-things/ (accessed 25 October 2015).
[39] Singleton, S. M. & Harper, J. (2001) 'With a grain of salt: What consumer privacy surveys don't tell us', SSRN 299930.
[40] Smith, H. J., Dinev, T. & Xu, H. (2011) 'Information privacy research: An interdisciplinary review', *MIS quarterly*, Vol. 35, No. 4, pp. 989-1016.
[41] Smith, H. J., Milberg, S. J. & Burke, S. J. (1996) 'Information privacy: Measuring individuals' concerns about organizational practices', *MIS quarterly*, pp. 167-196.
[42] Solove, D. J. (2006) 'A taxonomy of privacy', *University of Pennsylvania law review*, pp. 477-564.
[43] Spiekermann, S., Grossklags, J. & Berendt, B. (2001) 'E-privacy in 2nd generation E-commerce: Privacy preferences versus actual behavior', *Proceedings of the 3rd ACM conference on Electronic Commerce*, pp. 38-47.
[44] Stone, E. F. & Stone, D. L. (1990) 'Privacy in organizations: Theoretical issues, research findings, and protection mechanisms', *Research in personnel and human resources management*, Vol. 8, No. 3, pp. 349-411.

[45] Vargo, S. L. & Lusch, R. F. (2004) 'Evolving to a new dominant logic for marketing', *Journal of marketing*, Vol. 68, No. 1, pp. 1-17.
[46] Venkatesh, V., Thong, J. Y. & Xu, X. (2012) 'Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology', *MIS quarterly*, Vol. 36, No. 1, pp. 157-178.
[47] Warren, S. D. & Brandeis, L. D. (1890) 'The right to privacy', *Harvard law review*, pp. 193-220.
[48] Wellman, B. (2010) 'The reconstruction of space and time: Mobile communication practices', *Contemporary Sociology: A Journal of Reviews*, Vol. 39, No. 2, No. 179-181.
[49] Westin, A. F. (1967) *Privacy and freedom*, Athenaum, New York.
[50] Westin, A. F. (2003) 'Social and political dimensions of privacy', *Journal of social issues*, Vol. 59, No. 2, pp. 431-453.
[51] Weiser (1991) 'The computer for the 21st century', *Scientific American*, Vol. 56, No. 3, pp. 94-104.
[52] Xu, H., Teo, H. H., Tan, B. C. & Agarwal, R. (2009) 'The role of push-pull technology in privacy calculus: The case of location-based services', *Journal of Management Information Systems*, Vol. 26, No. 3, pp. 135-174.
[53] Yoo (2010) 'Computing in everyday life: A call for research on experiential computing', *f*, Vol. 34, No. 2, pp. 213-231.