2009

Investigating the Value of Privacy in Online Social Networks: Conjoint Analysis

Hanna Krasnova
Humboldt-University, Berlin, krasnovh@wiwi.hu-berlin.de

Thomas Hildebrand
European School of Management and Technology, hildebrand@e-ca.com

Oliver Guenther
Humboldt-University, Berlin, guenther@wiwi.hu-berlin.de

INVESTIGATING THE VALUE OF PRIVACY IN ONLINE SOCIAL NETWORKS: CONJOINT ANALYSIS

Completed Research Paper

Hanna Krasnova
Humboldt-Universität zu Berlin
Institute of Information Systems
Spandauer Str. 1, 10178 Berlin, Germany
krasnovh@wiwi.hu-berlin.de

Thomas Hildebrand
European School of Management and Technology
Schlossplatz 1, 10178 Berlin, Germany
thomas.hildebrand@esmt.org

Oliver Günther
Humboldt-Universität zu Berlin
Institute of Information Systems
Spandauer Str. 1, 10178 Berlin, Germany
guenther@wiwi.hu-berlin.de

Abstract

Popularity of Online Social Networks has been recently overshadowed by the privacy problems they pose. Users are getting increasingly vigilant concerning information they disclose and are strongly opposing the use of their information for commercial purposes. Nevertheless, as long as the network is offered to users for free, providers have little choice but to generate revenue through personalized advertising to remain financially viable. Our study empirically investigates the ways out of this deadlock. Using conjoint analysis we find that privacy is indeed important for users. We identify three groups of users with different utility patterns: Unconcerned Socializers, Control-conscious Socializers and Privacy-concerned. Our results provide relevant insights into how network providers can capitalize on different user preferences by specifically addressing the needs of distinct groups in the form of various premium accounts. Overall, our study is the first attempt to assess the value of privacy in monetary terms in this context.

Keywords: Online Social Networks, Web 2.0, Value of Privacy, Conjoint Analysis, Cluster Analysis

Introduction

Online Social Networks (OSNs) such as Facebook or StudiVZ represent popular Internet platforms that connect people around the globe. More than 250 million people are currently actively using Facebook with an average member having 120 friends (Facebook 2009). The value of OSNs lies in facilitating communication between users. By offering new easy ways to maintain relationships with offline contacts, OSNs may represent a key to solving the "bowling alone" problem, which manifests itself in increased disconnectedness and isolation of individuals in modern societies (Putman 2000). Indeed, OSNs allow individuals to support connection to other people, even if they are physically remote. This helps to create social capital, which can be viewed as a direct contribution of OSNs to public value (Ellison et al. 2007).

Despite their ability to create value, OSNs are often criticized for the privacy risks they involve. OSN providers, in particular, are often placed in the centre of this critique due to their questionable practices of using member information for commercial purposes (e.g. Schonfeld 2007). Many users regard *personalized advertising* as a privacy breach and express their privacy concerns in numerous OSN groups and personal blogs (Blakely 2007; Lischka 2007). More than one third of the articles in the review of German media by Rizk et al. (2009) related privacy violations to *personalized advertising* and *behavior targeting* - practices often traced back to OSN provider.

Addressing this set of concerns, it is important to note, however, that *using* information provided by users for marketing purposes may represent an important source to finance operations of OSNs, which are currently offered to users for free. This is because providing OSN service is costly. For example, StudiVZ (2009a), a popular German OSN, expands on the effort it takes to support the network: "*Our servers ensure that the data is available to you at the speed of 5.400 MBit per second during the peak times. As a comparison: a regular DSL-connection reaches 16 MBit/s. So, we are 338 times "faster"* (translated from German by the authors). As a result, many OSN providers will have little choice but to generate revenue through advertising in order to remain financially viable as long as the network is offered for free. Moreover, taking into account the low attention users pay at online advertising, personalization of banners might be the only real possibility to ensure sufficient money influx (Sachoff 2008). Therefore, even though a growing number of privacy abuse accusations are detrimental to OSN image, most of the criticized practices *will persist if the business model of OSNs remains unchanged*.

Despite the fact that users enjoy using their OSNs for free, OSN providers find it difficult to avoid critique from multiple stakeholders whenever they try to directly profit from their main asset - user information. For example, an attempt of StudiVZ to change their general terms and conditions in order to gain more rights with respect to using member data has triggered an outburst of discussions in the media. As a result, many users faked their profiles and some have even left the network. Similarly, Facebook has attempted to profit on social recommendations for consumer products by launching the Beacon application. Its introduction has resulted in an immense public outrage blaming Facebook for trying to misuse sensitive user data. History of these public failures transmits an important message to OSN providers: attempts to recklessly generate revenue without accounting for user privacy concerns can seriously undermine platform self-sustainability and result in a serious public backlash.

This type of dynamics places OSN provider in front of a problem, which is hard to solve. Moreover, users are getting increasingly vigilant with regard to their OSN activities as a consequence of perceived privacy threats (e.g. Krasnova et al. 2009). Despite their concerns, users have, however, only one "take-it-or-leave-it" option when joining an OSN. Even if they are not comfortable with the terms and conditions, e.g. use of their information or availability of privacy controls, users have no choice but to comply or stay out of the game. Being continuously dissatisfied with the way their privacy concerns are addressed, OSN users may choose to restrict their networking activities – an outcome in which all participating parties will lose. Moreover, public value of OSNs, expressed in their ability to create social capital, can be endangered.

Bringing both sides of the argument together, one can see that both parties - OSN providers and OSN users - find themselves as prisoners in a deadlock situation. On the one hand, users resent questionable information handling procedures, on the other hand OSN providers are left with no option, but to use some of member information to generate revenue, as long as the network is offered for free. This situation, however, can be changed. For example, business online networks such as Xing are already offering premium accounts, where no advertisements are displayed, users have a possibility to send more secure messages to other members and are offered more control over who visits their profiles (Xing 2009). Indeed, offering users to pay for their privacy may represent a viable solution out of the existing impasse.

This leads us to the following questions: Will OSN users be ready to pay for their privacy on the platform? And if so, how much? Are users ready to trade off some of their privacy in exchange for other incentives? To what extent and why do users differ in their privacy valuations? Finding answers to these questions will allow OSN providers to decide whether introducing premium "privacy-friendly" accounts constitutes a viable alternative to the current business model.

To address these research questions, we employ conjoint methodology, which is an accepted approach to measure consumer preferences in the light of the existing trade-offs. In fact, in a real situation users might be ready to trade their privacy for other benefits (Hui et al. 2006). This way a real privacy valuation can be derived. In the context of our study, we identify five variables playing a role in a user decision to choose an OSN: price, network popularity, profile customizability, availability of privacy controls and level of information use by the OSN provider. We then determine the importance of these variables in a user decision to join an OSN. In the next step, we employ hierarchical cluster analysis to segment OSN users into 3 groups in order to better understand how distinct segments of OSN users can be addressed (e.g. when designing a structure of premium accounts). Taken together, our study provides important insights on the real value of privacy on OSNs as well as gives valuable recommendations for OSN providers who can then create a more sophisticated revenue model by simultaneously addressing user privacy needs.

Related Work

Boyd and Ellison (2007) define OSNs as web-based services that allow individuals to create a profile and connect to friends within a bounded system. Hogben (2007) mentions development of the sense of connectedness and intimacy as an important benefit OSNs provide. In addition, OSNs enable users to control the impression they produce on others by allowing them to decide how much they are willing to self-disclose as well as by offering privacy settings to strategically manage access to personal information. On the *negative* side, privacy risks and resulting concerns are often mentioned as impediments to user participation and self-disclosure on OSNs (Krasnova et al. 2009).

Research provides multiple insights on the factors underlying the process of the formation of individual privacy preferences. From an organizational standpoint, violation of distributive justice principles reflecting the "*fairness of the outcome that they [users] receive from online companies in return for releasing their personal information*" (Son and Kim 2008, p. 510) can negatively impact users' feelings related to privacy loss (e.g. Culnan and Bies 2003). In addition, such environmental facts as trust in legal assurances may ultimately be correlated with individual privacy concerns (Krasnova and Veltri 2010). Personal experiences and individual predispositions may play a role as well. For example, Metzger (2004) argue that past levels of self-disclosure are predictive for future behavior. Furthermore, personal attitudes towards advertising and personalization (Phelps et al. 2001), general privacy attitudes (Joinson et al. 2006) as well as user trusting beliefs (e.g. Jarvenpaa and Tractinsky 1999) may influence the way people perceive risks related to a particular technology. Finally, demographic characteristics such as age and gender may determine individual privacy valuation (Sheehan 1999).

Typically, Privacy Calculus paradigm (Dinev and Hart, 2006) is used to explain the dynamics underlying user participation in the light of privacy concerns. This theory argues that when making a decision, individuals are consciously weighting costs (e.g. giving up privacy) and benefits (e.g. social connection (Joinson 2008) of their actions. Hence, users face certain trade-offs. What choice users make depends on their preferences. Privacy Calculus approach has been frequently applied using the Structural Equation Modeling methodology, where the model is assessed on the basis of the answers collected in a survey (e.g. Dinev and Hart 2006). However, Harper and Singleton (2001, p.1) argue that "*It costs a consumer nothing to express a desire for a law to protect privacy*". Consequently, survey instruments cannot help answer the question how much people will be ready to pay for their privacy in a real-life situation. These drawbacks of traditional surveys can be addressed by using conjoint analysis, which allows approximating consumer responses to a real-life setting with its inherent trade-offs.

Several researchers have already used conjoint analysis to study individual privacy valuation and its antecedents. Investigating consumer privacy concerns when information is collected by a marketer, Phelps et al. (2001) find that consumers' purchase decisions are determined by privacy concerns, which are, in turn, influenced by attitudes toward direct marketing and consumer desire for control over their personal information. In the next step, Hann et al. (2002) explore the trade-offs between three types of privacy concerns (errors, improper access and secondary use) and two types of benefits (monetary rewards and time savings) online consumers face when visiting a website. They confirm the presence of privacy calculus in individual decisions showing that users are willing to give up some of

their privacy for economic incentives. Extending that study, Hann et al. (2007) discover several clusters of users with similar utility patterns: privacy guardians, information sellers, and convenience seekers. The authors argue that companies have the means to address privacy concerns of their online consumers. Whereas offers of privacy protection against various types of privacy abuse are related to positive valences, they are capitalizable. This conclusion is important in the context of our study as OSN providers are currently looking for ways to mitigate user concerns as well as to ensure their financial survival.

Overall, insights into privacy preferences of OSN users are still sparse and are mainly derived on the basis of surveys involving Likert or similar scales, responses to which may be biased. Trying to fill this gap, we apply conjoint approach to understand the valuation of privacy by OSN users. This approach will help us to understand what choices users would make when facing different trade-offs, including privacy-related decisions. Overall, the use of conjoint analysis will help us to disentangle the existing puzzle on how the two opposing perspectives of OSN providers and OSN users can be reconciled.

Research Framework

In a conjoint analysis, it is assumed that consumers view products as a bundle of certain characteristics (attributes), which can take the form of different values (levels). For example, if "information use by OSN provider" constitutes an attribute of an OSN, the respective levels will be the different degrees of to what extent this information can be used (Orme 2002a). Conjoint analysis allows researchers to make inferences about the underlying value system (Johnson 1974) by allowing to decompose the overall utilities of the different stimuli consumers are asked to evaluate (in our case variations of OSNs). This way the relative importance of product attributes can be evaluated.

Pre-study: Interview Phase

To determine the attributes and their levels, we first analyzed the literature dealing with OSN participation and privacy trade-offs as described above. In the next step, as suggested by Green and Krieger (1991), we conducted multiple in-depth semi-structured interviews with OSN users in order to determine the main drivers of utility of OSNs[1]. This intermediate step helped us to reduce the danger of model misspecification since in Conjoint Analysis it is essential that no attribute driving users' utility is omitted from the analysis (Hair et al. 1995).

Interview participants singled out *presence of friends (network popularity)* and *profile customizability* as the key factors underlying OSN utility. These findings are in line with Boyd (2007, p.11) who notes that user behavior in OSNs is to a large extent determined by the desire to communicate and self-present: "*Through profiles, teens can express salient aspects of their identity for others to see and interpret*". While presence of one's friends satisfies the desire to communicate, profile customizability helps to self-express and self-present. Further, respondents mentioned *privacy-related factors*, such as *availability of privacy controls* as well as *practices of the OSN provider with respect to their information* (*Information Use by OSN Provider*) as important for their network use. These findings are in line with previous research results which show that users consider available privacy controls as insufficient (Boyd 2008) or too complex (Strater and Richter 2007) as well as resent misuse of their information by OSN provider (Rizk et al. 2009). These four factors were included as attributes into our model. In addition, in line with the purpose of our study, another attribute – *price* – has been integrated. Overall, these *five* attributes, *price, network popularity, customizability, information use by OSN Provider and privacy control*, have been considered. Note that this meets the recommendation by Green and Srinivasan (1990) that the number of attributes should be limited to at most 6.

The interviews also helped us to find appropriate levels for these five attributes. For example, we found that the fee of 10 Euro per month is unacceptable in the OSN context. A price of 6 Euro, similar to the one charged by Business Online Networks (e.g. Xing), has been mentioned as realistic. Further, when talking about the use of information by the OSN provider, respondents differentiated between the use of their *demographic* data and *all* information they provide. In addition, the levels for network popularity were chosen in line with Liehr (2005).

[1] Sample description of the interviewees and detailed discussion of the results of the interviews go beyond the scope of this paper and are available from the authors upon request.

Conjoint Design

Before starting the conjoint part of the survey, participants were provided with a set of instructions. Since we aimed to understand participants' choices independent of their current OSN membership we asked them to imagine that: (1) they were *not* a member of any OSN *yet*, (2) they were in the *process of choosing a network* that suited their preferences best and (3) they planned to sign in to the chosen network *under their real name*. At the next step, participants were instructed that OSNs could differ in five attributes, which were then presented together with their respective levels. Intuitive names were chosen for each level to ease understanding during the conjoint phase. Table 1 shows how the attributes and their respective levels were presented to the survey participants. These instructions were carefully pretested to ensure that respondents correctly remembered and interpreted each level.

Table 1. Explanation of Attributes and Levels

Attribute Name	Explanation of the Attributes and Levels given to Study Participants
Price	For now, almost all Social Networks are free, even though their maintenance is expensive. Their existence is often supported through online advertising (banners). In our scenarios, you can be required to pay for the OSN membership. The following levels of price are available: **Free: 0 Euro per month; 3 Euros per month; 6 Euros per month**.
Network Popularity	Some networks are big; others are rather small and specialized. In our scenarios, the OSN can have the following popularity among your friends and acquaintances: **25%; 50% or 75% of your friends/acquaintances are on the OSN.**
Customizability	OSNs may differ in the extent to which you can customize your profile (e.g. change page wallpaper, colors, fonts, and layout; add applications, favorite music, videos). In our scenarios, you have the following levels of customizability: • **Low Customizability:** The OSN offers little possibilities to distinguish your profile from others. You can only enter your personal information into the pre-designated fields. All profiles look more or less the same. *Example: StudiVZ* • **Medium Customizability:** You can customize your profile in terms of the look (wallpaper, text color, fonts) and applications, but the basic layout structure stays the same for everybody. • **High Customizability:** The OSN offers you many possibilities to create a visually unique profile. You are given a great flexibility in how the page can be structured (layout, wallpaper, font). Your profile is unique! *Example: MySpace*.
Privacy Control	OSNs may differ in the degree of privacy control options given to you. Privacy control options allow you to define who can access your information (profile, wall, photos, etc.). In our scenarios, you have the following choices: • **"ALL-OR-FRIENDS-ONLY**": In this scenario you are given one basic option: you can choose to show the profile to ALL users in the network OR to FRIENDS ONLY. • **"GROUP-BY-GROUP"**: In addition to the ALL-OR-FRIENDS-ONLY level, you can classify friends into groups of your own choice and specify which PARTS of your profile (e.g. photos, Wall) the different groups can or cannot see. *Example:* You may create a group called "Colleagues" which will not have access to all your pictures. • **"FRIEND-BY-FRIEND"**: In addition to ALL-OR-FRIENDS-ONLY and GROUP-BY-GROUP options, one can specify which ELEMENTS of your profile PARTS (a single photo in a photo-album) a particular FRIEND can or cannot see. *Example:* You have some party photos and would like friend X not to see two pictures from this particular party album. In this scenario you may forbid friend X access to these two pictures. Friend X will not know he does not have access to it.
Information Use by OSN Provider	Maintaining an OSN has its price. To finance itself, the OSN Provider may use some of the information you provide to display personalized advertising to you (e.g. banners). Generally, your information could be divided into two groups: **Demographics Information**

	(*age, gender, city, study major)* and **Personal Information** (*work, hobbies, personal interests, religion, political orientation, groups, relationship status, sexual orientation, photos, videos).* In our scenarios, you have the following choices: • **"NO INFORMATION IS USED"**: None of your Information is used. • **"ONLY DEMOGRAPHICS IS USED"**: Only your Demographic Information is used by the SN provider to personalize advertising displayed to you. *Example*: Women will be shown the advertising of the lipstick, whereas men the advertising of the new shaving gel. • **"ALL INFO IS USED"**: Your Demographic and Personal Information can be used by the OSN Provider to personalize advertising displayed to you. *Example*: Single men under 35 living in Stuttgart will be shown the advertising of a popular city club.

Survey Design: Complementary Part

Conjoint analysis is typically followed by a cluster analysis that aims to segment people into groups with similar utility patterns. In order to be able to better understand the factors underlying these differences in valuation across the resulting segments, we also asked respondents to provide their demographic information (e.g. sex) in a complimentary survey part. In addition, respondents were asked a set of questions measuring several constructs (see Table 2), which emerged as important determinants of individual privacy concerns, as outlined in the 'Related Work' section. We relied on existing operationalization where possible. However, many items had to be modified to fit OSN specifics. Most items were anchored on a 7-point Likert scale (1=Strongly Disagree; 7=Strongly Agree)[2].

Table 2. Examples of Construct Operationalization

Construct	No of items	Example of Items
Participation	3	1. I regularly log in on my OSN; 2. Using Social Network is part of my daily routine; (based on Ellison et al. 2006).
Amount of Self-Disclosure	4	1. I have a detailed profile on the Social Network I use; 2. My profile tells a lot about me; (based on Krasnova et al. 2009).
Legal Trust	3	1. I feel confident that existing laws protect me against abuse of my information online; 2. Existing laws adequately protect my information online; (based on McKnight et al. 2002).
Trust in online companies	4	Generally, online companies: 1. …are honest with users when it comes to using their information; 2. …are trustworthy in handling the information users provide; (based on Malhotra et al. 2004).
Distributive Justice	3	1. I find it fair that some of the information I provide can be used for personalized advertising in exchange for free social networking services; 2. The benefits I receive from OSN are attractive enough to let OSN provider use some of my information for marketing purposes. (self-developed)
Attention for Online Advertising	3	1. I don't pay attention to banners displayed on the websites; 2. I don't notice the banners when I am surfing on the Internet. *(Reversed)* (self-developed)
Attitude Personal. Advertising	4	How would you feel if online advertisings (e.g. banners) displayed to you on an OSN: 1…were adapted to your tastes; 2…were related to things of interest to you. (based on Chellappa and Sin 2005) (1=Very Bad; 7=Very Good)
Past Experience	3	How often have you felt in the past: 1. …that your privacy was invaded online? (based on Smith et al. 1996) (1=Never; 4=Sometimes; 7=Very Often)
Privacy Attitude	3	Privacy Segmentation Questions from Harris Interactive (2003)

[2] Complete list of items is available from the authors upon request.

Study Realization

There are several ways in how conjoint analysis can be conducted. When applying the traditional full-profile approach, researchers provide respondents with a set of stimuli which they have to rank or rate (e.g. Hann et al. 2002, 2007). Despite the fact that this approach is wide-spread, it represents a very high cognitive challenge to the respondents (Green and Srinivasan 1978) even when used in its reduced form (fractional factorial design). We tested the applicability of this approach by offering 20 students to rate 16 cards each with one stimulus (obtained from an orthogonal design of our 3 x 3 x 3 x 3 x 3=243 stimuli). We noticed that many students were struggling with the answers. Moreover, participants tended to dichotomize their responses, mainly concentrating on the 'price' attribute (free vs. not free). As a result, many responses were difficult to interpret and mostly unusable.

To avoid these problems, we decided to use computer-aided Adaptive Conjoint Analysis (ACA), which is a variant of the hybrid conjoint analysis implemented in the Conjoint Extension of the Globalpark Survey Suit (Globalpark 2008). A specific feature of the Adaptive Conjoint Analysis is that for each respondent, the consecutive answers are taken into account and immediately used for a further development of the personalized questionnaire. As a result, mental load of the respondents, needed to determine the importance of attributes and attribute levels, is significantly reduced (Srinivasan 1997). Due to the methodology of the ACA, participants had to answer all questions which were asked. Following Johnson (1987) and Green et al. (1991), our ACA consisted of *four* phases. The *first* phase involved rating of the attributes. From these responses, best and worst levels were obtained for each attribute and for each respondent. In the *second* phase, respondents were asked to determine the importance of the difference between the best and worst levels for each attribute. For example the following question was asked: If two Online Social Networks only differed in the level of Monthly Fee, how important would the difference of 'Free' vs. '6 Euro' be to you (1=Not Important at All; 7=Very Important)? In the *third* phase, respondents had to do 12 pair-wise comparisons: they had to specify on a bipolar seven-point scale (1=Strongly Prefer OSN1; 7=Strongly Prefer OSN2), which of two OSNs presented to them they preferred. In the *fourth* phase ("calibration phase"), the participants were given five examples of Online Social Networks and for each of them had to indicate on a scale from 0 to 100 how much they were likely to join. The calibration phase is important since it allows assessing how attentive participants were when filling in the questionnaire. A negative or very small correlation between final utilities and calibrated utilities indicates that the respondent was inattentive to the questionnaire and / or responded inconsistently.

Analysis of Empirical Results

Sampling

Invitations to participate in the study were distributed via multiple mailing lists in numerous universities. The responses were collected from January until March 2009. About 50 % of the participants received a 5-Euro gift certificate in exchange for their participation. The overall gross sample consisted of 214 observations. After deleting 43 incomplete observations and 3 observations with low correlation between final and calibrated utilities, a final net sample had 168 observations. Being a current OSN member was not a precondition for this study. In total, however, 69% (19%) of the respondents stated that they used Facebook (StudiVZ) as their main OSN. Only 3 participants were not members of any network. The sample consisted to 60.7% of women. The majority of the respondents were either students or had a university degree. 85.7% (respectively 10.1%) were between 20 and 29 (respectively between 30 and 39) years old. 26.2%, 39.9%, 6.0% and 3.0% were coming from France, Germany, Russia and the United Kingdom, respectively. 17.3%, 72.6% and 10.1% belonged to Privacy Fundamentalists, Pragmatists and Unconcerned groups, respectively, according to the privacy segmentation by Harris Interactive (2003).

Analysis Structure

The analysis of the study results involved several stages. First, using conjoint analysis, the relative importances of our five attributes as well as final utilities (part-worths), reflecting the attractiveness of a specific attribute level, were derived. The relative importances allowed us to draw conclusions about the role each attribute plays in a user's decision to join the network. Part-worths were used to estimate the utility change between attribute levels and gave insights about the trade-offs users might consider. Further, Euro-values for each change in the attribute levels were derived, which gives OSN providers initial insights on how user preferences for certain attribute levels can be

translated into monetary value. While the first part of our analysis gave us an "average" picture of the way various attributes and their levels are valued by OSN users, in the second step we acknowledged that there may be systematic differences between various user sub-groups within our sample. As a result, 3 groups of people with similar utility patterns were derived with the help of a cluster analysis of the final utilities. We then analyzed the distinctive characteristics of these clusters by looking at the differences between the relative importances of various attributes, the utility change values as well as the Euro-values of level changes.

Analysis of Conjoint Results

Table 3 presents the results of the conjoint analysis: the average relative importance of the different attributes as well as the average mean final utilities (part-worths)[3] of the corresponding levels for the overall sample. Column "Utility change" of Table 4 depicts the average change in final utility if the network switches from one level of an attribute to another one. Column "P-value on equality" of Table 4 shows the P-value on the t-test conducted on the null hypothesis that the two levels provide the same utility for the users (equal average part-worths). Relative importances were calculated on the basis of the part-worths. In accordance with Orme (2002b) we averaged individual relative importances for respondents for the overall sample, rather than computing importances from averaged utilities. Relative importances help us to understand the ranking of the attributes when it comes to the choice of an OSN.

Studying the results, note that if we consider the different attributes independently from each other, all final utilities have the expected relations. Looking at the highest part-worth for each attribute we can derive the ideal OSN from the user point of view: it is free, includes 75% of one's friends (the more the better), allows to restrict accessibility on the friend-by-friend basis, no user information is used and customizability is either medium or high.

With a relative importance of 31.1%, *price* is the most important factor in the choice of an OSN. The P-values of the tests on equality of part-worths indicate that all price levels provide significantly different utilities. We observe that utility decrease is bigger for a change of price from "free" to "3 Euros" than from "3 Euros" to "6 Euros" (see Table 4). This indicates a particular aversion to a shift from a free network to a paid one. *Network popularity* is the second most important variable: the relative importance constitutes 24.7%. We find that utility is increasing in network size, yet a change from "25%" to "50%" is more valuable than from "50%" to "75%", which may hint at decreasing marginal utility of network popularity. Our results demonstrate how much value users attach to this attribute. Imagine two competing networks: one with 75% and one with 25% in popularity with other things being equal. The more popular network could increase its price from € 0 to € 3 Euro for its service (absolute utility drop of 2.107) without being afraid to immediately lose its user base, as the absolute drop in utility when switching to the less popular network (75% to 25% in popularity) would still be higher (1.665 + 1.344 = 3.009). *Information Use by OSN Provider* plays an important role, too: The relative importance of this attribute amounts to 18.7%, so that this criterion is the third most important factor, even outpacing customizability and privacy control. This finding refutes the common notion that OSN users do not care about their privacy, which is in line with Krasnova et al. (2009) findings who confirm a link between privacy concerns and resulting behavior. As expected, utility is higher the less information is used (see Table 3). Note that the utility decrease from "no information used" to "demographic data used" is far less pronounced than that from "demographic information used" to "all information used", showing that OSN users are particularly alerted if a network uses all their personal information. A closer look at our results shows that users are almost indifferent between (1) paying for the OSN if it increases its price from € 0 to € 3 and does not use their information (absolute utility drop of 2.107) and (2) paying nothing but letting the OSN provider use *all* their information instead of no information (-0.829 + -1.468 = -2.297 ≈ -2.107) with all other things being equal. This is an important finding, as it shows that, contrary to the popular claims that "OSNs should be for free" or that "privacy is priceless", there exists a distinct market for privacy. This finding is in line with Hann et al. (2002), who also shows that users are ready to sacrifice some of their privacy for monetary benefits. With 13.9%, *privacy control* has a rather low relative importance. This finding may be indicative for the low perceived effectiveness of privacy controls in protecting published information against many types of abuse. Indeed, regardless of the chosen privacy setting, OSN providers still have access to user data. Moreover, approved contacts can also make published information available to unauthorized others. Nevertheless, more control is perceived as better by the users. This is

[3] Note that in our Adaptive Conjoint Analysis we used "effects coding", which means that utilities are scaled to sum to 0 within each attribute. Consequently, it is not appropriate to test whether the average final utilities are statistically different from 0 and, therefore, we do not provide P-values on this test.

in line with Phelps et al. (2001), who show that consumers' desire for control over their personal information is an important factor in reducing privacy concerns. Thus, users are not afraid of complexity with regard to privacy settings and are ready to take effort to deal with intricate privacy design in exchange for more refined access controls. Finally, *customizability* also has a low relative importance (11.5%). Here, it is noteworthy that users almost do not perceive any difference between "medium customizability" and "high customizability" (the corresponding P-value equals 0.637, Table 4). In line with this finding, Facebook does not have to invest more into a more flexible profile design. In fact, it offers optimal page customizability (medium), by allowing users to always keep their profiles different (by posting comments, photos, website links on the Wall), but within a specified standard structure (basic layout).

Table 3. Attributes, Levels, Relative Importances and Final Utilities

Attributes	Levels	Final Utilities (Part-Worths)	Standard Errors	Relative Importances
Price	Free	1.981	0.049	31.1%
	€ 3	-0.126	0.042	
	€ 6	-1.855	0.043	
Network Popularity	25% of friends	-1.558	0.055	24.7%
	50% of friends	0.107	0.034	
	75% of friends	1.451	0.055	
Customizability	Low	-0.489	0.056	11.5%
	Medium	0.225	0.039	
	High	0.264	0.058	
Privacy Control	All-Or-Friends-Only	-0.410	0.071	13.9%
	Group-By-Group	-0.030	0.057	
	Friend-By-Friend	0.440	0.066	
Information Use by OSN Provider	None	1.042	0.054	18.7%
	Only demographics	0.213	0.037	
	All	-1.255	0.057	

From Table 4 we observe that the total change in final utility from "3 Euros" to a free network implies a change of 2.107/3=0.702 units of final utility per Euro. Correspondingly, we calculate the final utility change per Euro for a change from "6 Euros" to "3 Euros" with 1.730/3=0.577 units. We thereby obtain an *upper and a lower bound* for the utility change per Euro. These bounds can then be used to calculate the Euro equivalent of a change in the levels of the other attributes considered in our study (Table 4, columns "Euro value of change"). For example, a change from a network with 25% of the friends to one with 50% of the friends is worth the equivalent of between 2.372 Euros and 2.888 Euros per month. Changing network popularity from 50% to 75% is worth between 1.914 and 2.331 Euros. Similarly, users would pay about 1 Euro per month for a change from a network with low customizability to one with medium customizability, whereas on average additional high customizability is worth less than 10 additional Cents. Our results show that users are ready to pay between 0.669 and 0.815 Euro for the possibility to control access to their information on a Friend-By-Friend basis as opposed to a Group-By-Group basis. For the possibility to limit the use of their information from "all info" to "only demographic info" users would pay between 2.091 and 2.546 Euros. Finally, for an additional change to "no info" they would pay an additional 1.180 to 1.437 Euros. Assuming that a network of the size of StudiVZ (6 million members (StudiVZ 2009b), were using only demographic information to personalize advertising, it could earn between € 85.0 and € 103.4 a year (Euro value of change x 6 million members x 12 months) by declaring that it is not going to use any information for personalized advertising. Of course, this amount has to be reduced by the corresponding loss in personalized advertising revenue. Nevertheless, this size of potential income is impressive. For example Facebook, a network of much bigger size which places higher emphasis on personalization and user targeting, was able to generate only $150 million in

revenue in 2007 (Schonfeld 2008). Overall, these results show that OSN providers can capitalize on user preferences. It is important to note, however, that there might be systematic differences between various user sub-groups within our sample. Understanding these differences might lead OSN providers to derive relevant inferences about the structure of user preferences in various sub-groups and hence optimize its offerings.

Table 4. Utility Change and Euro Value of Change

Attribute Name	Level Change	Utility Change	P-value on Equality (t-test)	Euro Equivalent of Level Changes (Bound 1 – Bound 2)
Price	Free → € 3	-2.107	0.000	
	€ 3 → € 6	-1.730	0.000	
Network Popularity	25% → 50% of friends	1.665	0.000	-2.372 – -2.888
	50% → 75% of friends	1.344	0.000	-1.914 – -2.331
Customizability	low → medium	0.715	0.000	-1.018 – -1.239
	medium → high	0.039	*0.637*	-0.056 – -0.068
Privacy Control	All-Or-Friends-Only → Group-By-Group	0.380	0.001	-0.540 – -0.658
	Group-By-Group → Friend-By-Friend	0.470	0.000	-0.669 – -0.815
Information Use	none → only demographics	-0.829	0.000	1.180 – 1.437
	only demographics → all info	-1.468	0.000	2.091 – 2.546

Cluster Analysis of Final Utilities

In the next step, we conducted a Hierarchical Agglomerative Cluster Analysis on the respondents' individual final utilities in order to determine groups of people with similar utility patterns. The Ward's linkage we applied forms groups by evaluating the distances between clusters on the basis of an analysis of variance (ANOVA) approach: Starting from as many clusters as there are observations in the sample, at each clustering step the algorithm minimizes the sum of squares of the two clusters which are merged. From the resulting dendrogram we concluded that OSN users in our study can be divided into 3 major clusters with 49 (29.1%), 63 (37.5%) and 56 (33.3%) users in each cluster, respectively. Table 5 shows the corresponding relative importances (RI) and Table 6 reflects differences in the utility changes across clusters.

Table 5. Relative Importances (RI) by Cluster

	Relative Importances			P-values			
	Cluster 1	Cluster 2	Cluster 3	F	t-test Cluster 1/2	t-test Cluster 2/3	t-test Cluster 1/3
Price	37.5%	26.5%	30.7%	0.000	0.000	0.003	0.000
Network Popularity	27.3%	28.7%	18.0%	0.000	*0.483*	0.000	0.000
Customizability	12.9%	11.5%	10.4%	*0.242*	*0.370*	*0.369*	*0.096*
Privacy Control	12.3%	16.1%	12.7%	0.012	0.006	0.022	*0.776*
Information Use	9.9%	17.1%	28.2%	0.000	0.000	0.000	0.000

From Table 5 we can derive that participants in *cluster 1* place particular weight on *network price* (RI=37.5%). Table 6 shows that these users are particularly adverse to a change in price from Free to € 3. High *network popularity* also plays an important role in the decision of users in cluster 1 to choose an OSN (RI=27.3%). Moreover, this group cares *the least about the use of their information* by the OSN provider (RI=9.9%). Offering

these users not to use their information for personalized advertising is by far not enough to make them pay for OSN services: Their aggregated drop in utility between "none info is used" and "all info is used" is more than 2 times lower than their utility decrease when price is changed from Free to € 3. In its essence, this group seems to uphold the traditional opinion that OSNs should be offered to users for free. Users in this cluster also seem not ready to invest their time and effort to deal with an increasing complexity of the privacy settings and view them rather as hindering than useful. In contrast to other groups, users in cluster 1 consider changes in privacy control from All-Or-Friends-Only to Group-By-Group as negative (see Table 6). For participants in cluster 1, even customizability was more important (RI=12.9%) than availability of privacy controls (RI=12.3%) or use of their information by the OSN provider (RI=9.9%). Based on these characteristics we call this cluster "Unconcerned Socializers". In their core, they are oriented to extract a maximum interaction value from the network at the lowest cost and without accounting for long-term privacy risks. The fact that 29.1% of the respondents in our sample upheld this set of views regarding their privacy on OSNs shows that the share of people unconcerned about their privacy on OSNs is slightly higher than it was found in other contexts. For example, 23% were 'unconcerned' about their online privacy in a study conducted by Jensen et al. (2005) and only 20.51% belong to the "information sellers" cluster identified by Hann et al. (2007) for the US respondents.

Table 6. Utility Change by Cluster

	Utility change by clusters			P-value			
Level change of the attribute	Cluster 1	Cluster 2	Cluster 3	F-test	t-test Cluster 1/2	t-test Cluster 2/3	t-test Cluster 1/3
Price							
Free → € 3	-2.419	-1.868	-2.101	0.023	0.006	*0.220*	0.103
€ 3 → € 6	-1.683	-1.765	-1.731	*0.882*	*0.618*	*0.846*	*0.782*
Free → € 6	-4.102	-3.633	-3.833	*0.061*	0.022	*0.320*	*0.127*
Network Popularity							
25% → 50% of friends	1.663	2.089	1.191	0.000	0.008	0.000	0.006
50% → 75% of friends	1.292	1.790	0.888	0.000	0.002	0.000	0.016
25% → 75% of friends	2.954	3.879	2.079	0.000	0.000	0.000	0.000
Customizeability							
low → medium	0.700	0.875	0.548	*0.203*	*0.355*	*0.075*	*0.425*
medium → high	*0.036*[ns]	*-0.207*[ns]	0.319	0.015	*0.268*	0.004	*0.156*
low → high	0.736	0.667	0.867	*0.706*	*0.809*	*0.419*	*0.620*
Privacy Control							
All-Or-Friends-Only → Group-By-Group	-0.648	0.839	0.762	0.000	0.000	*0.754*	0.000
Group-By-Group → Friend-By-Friend	*0.200*[ns]	0.955	*0.161*[ns]	0.001	0.002	0.001	*0.872*
All-Or-Friends-Only → Friend-By-Friend	-0.449	1.794	0.923	0.000	0.000	0.001	0.000
Information Use							
none → only demographics	-0.273	-0.794	-1.354	0.000	0.000	0.001	0.000
only demographics → all info	-0.688	-1.497	-2.119	0.000	0.000	0.000	0.000
none → all info	-0.961	-2.291	-3.473	0.000	0.000	0.000	0.000

ns: part-worth was not significant.

Cluster 2 is made up of users who place much more value than members of the two other clusters on the *ability to control* accessibility of the information they provide by using privacy settings (RI=16.1%). Table 6 demonstrates

that while for clusters 1 and 3 the utility change in privacy control from Group-By-Group to Friend-By-Friend is insignificant, for users in cluster 2 it is significant. This shows that users belonging to Group 2 are ready to make significant trade-offs to gain more refined control. Users belonging to cluster 2 also look for a particularly *large network* (RI of network popularity is 28.7%). Table 6 also reflects a particular sensitivity of this group to changes in network popularity. Furthermore, in contrast to the other groups, *price of the network* is of less importance for group 2 (RI=26.5%). Based on these findings, we call this cluster "Control-conscious Socializers".

Finally, users in *cluster 3* are – compared to users in the other two clusters – very concerned about their privacy: the way *how their information is used by the OSN provider* is particularly important for them (RI=28.2%). As Table 6 shows, all clusters demonstrate a drop in utility when the use of their information increases. However, for users in cluster 3 the utility drop for a change from "no info is used" to "only demographic information is used" is twice as high as for cluster 2 and five times higher than for cluster 1. In fact, people in cluster 3 would rather accept a higher price and especially a smaller network if, in turn, their information is not used. Indeed, *network popularity* (RI=18%) is not as important for this cluster as for the two other ones: Table 6 reflects only a very small utility increase when network popularity grows from 50% to 75%. Summarizing these results, we call this group "Privacy-Concerned". The fact that 33.3% of our respondents were part of the "Privacy-Concerned" category is in line with the findings from Jensen et al. (2005), who find that 34% of the respondents in his sample belonged to the group of people strongly concerned about their privacy – "Fundamentalists". However, based on conjoint analysis, Hann et al. (2007) assign 71.79% of US respondents to a "privacy guardians" cluster. Even though the share of this segment significantly exceeds the share of people in our "Privacy-Concerned" category, the total share of "Control-conscious Socializers" and "Privacy-Concerned", two groups with special privacy preferences identified in our study, comprises 70.8%, which is comparable to the results by Hann et al. (2007).

As described in the "Survey Design: Complementary Part" subsection, in addition to completing the conjoint part, participants were asked to answer a set of survey questions measuring various constructs as presented in Table 2. The answers to these questions were averaged to form an index for each construct. At the next step, for each construct index, we compared means over the three different clusters using an F-test on the equality of means. Where there was evidence that the means between the clusters differed, we additionally conducted t-tests on pair-wise comparison. Column "Significant pair-wise comparisons across clusters" of Table 7 shows for which clusters the means were significantly different from each other.

We find that in cluster 1 – "Unconcerned Socializers", who tend to be less concerned about OSN-related privacy issues – the share of men is the highest. This is in line with Sheehan (1999), who shows that women are more concerned about secondary usage of their information. On average, "Unconcerned Socializers" demonstrate a significantly higher level of *trust in legal assurances, online companies and have the lowest scores on the Privacy Attitudes scale.* This shows that these users tend to have stronger beliefs that their privacy is ultimately protected by law and hence they do not have to pay to protect their privacy – a risk already taken care of by policy-makers. And even if laws are not strong enough, these users trust that online companies are honest, predictable and consistent regarding the usage of the information they provide. In fact, Pavlou (2003) shows that trust plays a central role in reducing individual risk perceptions. Finally, "Unconcerned Socializers" show significantly less privacy concern on the Privacy Segmentation questions (Harris Interactive 2003).

In cluster 2 "Control-conscious Socializers", the share of women is significantly higher than both in cluster 1 and in the overall sample. This finding reveals that women are more likely to be interested in additional privacy controls on OSNs, which is a major characteristic of cluster 2. This is surprising, as men were previously found to have a higher desire for control than women, even though this difference was not confirmed in later studies (Burger and Solano 1994). On the other hand, this result may be reflective for the fact that women tend to disclose more on OSNs, by posting more photos or leaving more self-descriptive information (Kolek and Saunders 2008) and, hence, may need more control to protect themselves from the prying eyes of the unknown others. Supporting this argument, users in cluster 2 have the highest disclosure and OSN participation rates (although the difference between clusters 1 and 2 is insignificant). In addition, in contrast to female users, men tend to use OSNs to get to know new people (Tufekci, 2008b), which often implies leaving their profile information visible to others (Lampe et al. 2007). Confirming this logic, Tufekci (2008a) finds that men are more likely to leave their profile open on MySpace. Further, female users seem to be more appreciative of the network popularity, which is an important characteristic of cluster 2. Indeed, multiple research findings have confirmed a greater value women attach to the benefits of keeping in touch and social connection (e.g. Joinson 2008)

The share of women in cluster 3 "Privacy-Concerned" does not differ significantly from the overall sample. *"Privacy-Concerned"* users show less agreement with the distributive justice argument – that it is fair to use their information in exchange for the free networking services – in comparison to "Unconcerned Socializers". Users in this cluster tend to reveal significantly less information and also participate less on OSNs. Hence, existing privacy concerns seem to be indeed negatively related to user participation and self-disclosure. Taking into account that 33.3% of the users in our study belong to this group, this finding is relevant for OSN providers. It shows that if privacy concerns of this group are not addressed, these users might gradually minimize their OSN activities.

Interestingly, there is no significant difference in the declared privacy attitude between clusters 2 and 3. However, as our previous analysis shows, users in these two groups tend to address their privacy concern in two different ways. "Control-conscious Socializers" rely on privacy settings, whereas "Privacy-Concerned" prefer contractual agreements specifying how their information can be used. Furthermore, the clusters do not differ with regard to the privacy-related past experience of the users. Possibly, media coverage of privacy risks on OSCs is strong enough to make users learn from the mistakes of others: So that it makes no difference whether or not user privacy has actually been abused in the past. In addition, we find no difference between users across clusters with regard to the attention they pay to online advertising: on average all groups slightly agree with statements like: "I don't pay attention to banners displayed on the websites". Even though all three groups tend to equally "not notice" online advertising, "Privacy-Concerned" users show a slightly negative and "Unconcerned Socializers" a slightly positive attitude towards personalization. This is in line with the results of Wolin and Korgaonkar (2003), who find that males, predominating our cluster 1 "Unconcerned Socializers", tend to have more favorable attitudes towards online advertising when compared to magazine, newspaper or radio channels.

Table 7: Description of the Three Clusters in Terms of Additional Variables

Cluster	Cluster 1: "Unconcerned Socializers"	Cluster 2: "Control-conscious Socializers"	Cluster 3 "Privacy-Concerned"	Overall Sample	P-value ("H0: Means of the 3 clusters are equal")	Significant (at 5 %) pair-wise comparisons across clusters
Gender: Share of women	45.7%	75.8%	64.2%	63.3%	0.006***	1-2
Participation	5.592	5.608	4.786	5.329	0.021**	2-3; 1-3
Self-Disclosure: Amount	4.235	4.371	3.336	3.986	<0.001***	2-3; 1-3
Legal Trust	4.048	3.455	3.190	3.540	0.010***	1-2; 1-3
Trust in Online Companies	3.724	3.429	3.205	3.440	0.074*	1-3
Distributive Justice	4.293	3.989	3.542	3.929	0.069*	1-3
Attention to Online Advertising *(values reversed)*	3.626	3.726	3.685	3.683	0.928	
Attitude Personalized Advertising	4.381	4.339	3.815	4.177	0.064*	2-3
Past Experience	2.750	2.902	3.101	2.924	0.317	
Privacy Attitude	3.918	4.487	4.673	4.383	<0.001***	1-2; 1-3

*Significant at 10%, ** Significant at 5%, *** Significant at 1%

Detailed Analysis of Clusters – Euro Values

We now turn to the managerial interpretations of our study. Table 8 presents the Euro-values of level changes in the attributes for the 3 different clusters. These values were calculated in the same way as was described in the "Analysis of Conjoint Results" subsection of our study for the overall sample. We find that "Control-conscious Socializers" are ready to pay between € 1.360 and € 1.656 per month for more refined privacy settings (Group-By-Group → Friend-By-Friend), which makes it € 16.32 and € 19.87 per year. Taking into account that 37.5% of users belong to this group, a network as big as StudiVZ could earn between additional € 36.8 and € 44.7 million (6 million

members x 37.5% x € 16.32 or € 19.87) by offering a corresponding type of premium accounts to this specific group. Furthermore, "Privacy-Concerned" users (33.3%) are ready to pay on average between € 23.1 and € 28.2 (1.928 – 2.348 x 12) per year to ensure that their demographic information is not used for personalized advertising. They are followed by "Control-conscious Socializers", who are ready to pay between € 13.6 and € 16.5 (1.130 – 1.376 x 12) per year for this. "Unconcerned Socializers" are ready to pay only a fraction – between € 4.7 and € 5.7 (0.389 – 0.474 x 12) a year – to prevent the OSN provider from using their demographic information. Our analysis shows that from a commercial point of view, the OSN provider can capitalize the most on the users belonging to the "Control-conscious Socializers" group. Indeed, not only are these users ready to pay for enhanced privacy settings, but they are also ready to pay significantly large amounts to ensure that their information is not used. For example, if a network like StudiVZ offers a premium account with enhanced privacy controls and no demographic information used, it will be able to charge "Control-conscious Socializers" at least € 29.92 (€ 16.32 + € 13.6) a year. Another "cheaper" premium account can specifically target the "Privacy-Concerned" users, with "just" no demographic information being used at a price of € 23.1 a year. Even though a detailed analysis of possible tariffing goes beyond the scope of this paper, the interested reader can build an impression on how OSN providers can meet user privacy concerns and at the same time ensure a sustainable revenue influx.

Table 8 Utility Change per Euro and Euro Equivalent of Level Changes (Bound 1 – Bound 2)

	Cluster 1 "Unconcerned Socializers"	Cluster 2 "Control-conscious Socializers"	Cluster 3 "Privacy-Concerned"	Overall Sample
Utility change per Euro (Bound 1 – Bound 2)	0.806 – 0.561	0.623 – 0.588	0.700 – 0.577	0.702 – 0.577
Level change	Euro equivalent of level changes (Bound 1 – Bound 2)			
Network Popularity				
25% → 50% of friends	-2.368 – -2.883	-2.976 – -3.623	-1.696 – -2.065	-2.372 – -2.888
50% → 75% of friends	-1.840 – -2.240	-2.549 – -3.104	-1.264 – -1.540	-1.914 – -2.331
Customizability				
low → medium	-0.996 – -1.213	-1.246 – -1.517	-0.780 – -0.950	-1.018 – -1.239
medium → high	-0.051 – -0.063	0.295 – 0.360	-0.454 – -0.553	-0.056 – -0.068
Privacy Control				
All-Or-Friends-Only → Group-By-Group	0.923 – 1.124	-1.194 – -1.455	-1.086 – -1.322	-0.540 – -0.658
Group-By-Group → Friend-By-Friend	-0.284 – -0.346	-1.360 – -1.656	-0.229 – -0.279	-0.669 – -0.815
Information Use				
none → only demographics	0.389 – 0.474	1.130 – 1.376	1.928 – 2.348	1.180 – 1.437
only demographics → all info	0.980 – 1.193	2.132 – 2.596	3.018 – 3.675	2.091 – 2.546

Discussion and Concluding Remarks

Our study is the first attempt to empirically investigate the factors behind the choice of an OSN using a conjoint approach. We find that price and network popularity play the most important role in the user decision to join an OSN, with users showing a particular aversion to a shift from a free network to a paid one. This can be partially due to the fact that traditionally OSNs have been offered for free. Furthermore, in contrast to a widespread opinion concerning carelessness of OSN users with regard to their privacy, a factor *Information Use by OSN Provider* emerged as third in importance. Our results also show that enhanced privacy controls are appreciated by many users. These users are not afraid of complexity with regard to privacy settings and are ready to take an effort to deal with complexities of privacy design in exchange for more control over personal information. Finally, customizability emerged as the least relevant factor, with users not making a distinction between "high" vs. "medium

customizability" in terms of their utility. A particular advantage of conjoint analysis is that it allows to derive founded inferences concerning the value respondents attach to particular attribute levels. This approach differentiates our study from other survey-based attempts to evaluate user privacy concerns (e.g. Acquisti and Gross 2006). Our results show that on average a user would be ready to pay between € 14.14 and € 17.24 a year (12 months x € 1.180 – € 1.437) if the OSN provider refrained from using his or her demographic information for personalized advertising. For a network with a size of StudiVZ (6 million members (StudiVZ 2009b), this would mean an annual revenue of € 85.0 and € 103.4 – a sum comparable to StudiVZ market value of approximately € 100 million (Cubrilovic 2008).

Acknowledging that there might be systematic differences between users within our sample, we conducted a cluster analysis in order to determine groups of users with similar utility patterns. Knowledge about the existence of these clusters will allow OSN providers to design their offerings to target the specific needs of these groups (e.g. various premium accounts). We find three distinct clusters of OSN users: "Unconcerned Socializers", "Control-conscious Socializers" and "Privacy-Concerned" users. We show that importance attached to network popularity, price as well as preferences regarding one's own privacy underlie the differences across these clusters.

"Unconcerned Socializers", a male-dominated group, are willing to get the maximum communication value from the network at the lowest cost possible. Our complimentary analysis has revealed that users belonging to this group may rely on the legal system and therefore not see a reason to pay for their privacy. This finding is disturbing, taking into account the low level of user knowledge with regard to privacy regulation and OSN privacy policy (Acquisti and Gross 2006). Generally, the fact that the share of *"Unconcerned Socializers"* identified in our study is higher than the share of *"Unconcerned"* found in comparable surveys (e.g. Jensen et al. 2005; Hann et al. 2007) should be alarming for policy-makers and other stakeholders. It shows that users might be significantly underestimating the risks related to their participation on OSNs. In this regard, the role of policy-makers emerges as particularly important, as major effort is needed to ensure that users make rational decisions in the face of existing trade-offs. *"Control-conscious Socializers"* is a female-dominated group of users who are looking for a particularly *large network* and who place high value on the *ability to control* accessibility of the information they provide. Translating the value these users attach to their privacy into monetary terms, we find that a network of the size of StudiVZ could earn additionally between € 36.8 and € 44.7 million by offering more refined privacy settings specifically to this group. Finally, *"Privacy-Concerned"* users are very concerned about *how their information is used by the OSN provider*. On average, these users participate significantly less in OSN activities than users of the other two groups. OSN providers should pay a particular attention to this group: If their privacy concerns are not addressed, these users might minimize their activities on the platform. On the other hand, taking into account the high value these users attach to their privacy, the OSN provider could charge these users between € 23.1 and € 28.2 per year in exchange for not using their demographic information for personalized advertising. This way, the interests of both groups, OSN users and OSN provider, would be met.

Limitations and Further Research

Our study is subject to several limitations. First, a large part of our respondents were students. Taking into account the fact that the demographics of OSNs are constantly changing (insidefacebook.com 2009), further research should validate our findings with other population groups. In addition, most respondents in our sample have European origin, which limits the scope of our study to European user base. Krasnova and Veltri (2010), however, show that German and US users exhibit different attitudes when it comes to their level of privacy concerns on OSNs, trust in the OSN provider and legal assurances. Furthermore, differences in income may also have an impact on how much users are ready to pay for their privacy. Hence, validating our study results in other countries, including those with lower average income levels, e.g. China and India, represents a worthwhile venue for future research. Finally, the results of every conjoint analysis are highly dependent on the choice of the attributes and their respective levels. Therefore we are aware of possible disagreement on the choices we made. Addressing this argument we stress that all our decisions were based on the extensive literature review combined with pre-study interviews and careful pretesting of the conjoint design.

Acknowledgements

We would like to thank Yann and Laurène for their help in conducting this study.

References

Acquisti, A. and Gross, R. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook", in *Proceedings of 6th Workshop on Privacy Enhancing Technologies*, Golle, P., Danezis, G. (Eds.), Robinson College, Cambridge, 2006, pp. 36-58.

Blakely, R. "Facebook shrugs off privacy fears with plan for targeted advertising", 2007. http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2426470.ece. Accessed 30th April 2009.

Boyd, D. "Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence", *Convergence* (14:1), 2008.

Boyd, D. "Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life", in *Youth, Identity, and Digital Media,* Buckingham, D. (Ed.), MIT Press, Cambridge, MA, 2007, pp.119-142.

Boyd, D. and Ellison, N. "Social Network Sites: Definition. History. and Scholarship", *Journal of Computer-Mediated Communication* (13:1), 2007.

Burger, J.M., Solano, C.H. "Changes in desire for control over time: gender differences in a ten-year longitudinal study", *Sex Roles* (31), 1994, pp.465-72.

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

Cubrilovic, N. "Facebook Sues German Social Network StudiVZ", 2008. http://www.techcrunch.com/2008/07/18/facebook-sues-german-social-network-studivz/. Accessed 30th April 2009.

Culnan, M. J. and Bies, R.J. "Consumer privacy: Balancing economic and justice considerations", *Journal of Social Issues* (59:2), 2003, pp. 323-342.

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

Ellison N, Steinfield C, Lampe C. "The benefits of Facebook "friends:" Social capital and college students' use of online social network sites", *Journal of Computer-Mediated Communication* (12:4), article 1, 2007.

Ellison, N., Steinfeld, C., Lampe, C. "Spatially Bounded Online Social Networks and Social Capital: The Role of Facebook", *Annual Conference of the ICA*, Michigan State University, MI, 2006.

Facebook. Statistics. Press Center. http://www.facebook.com/press/info.php?statistics. Accessed 3rd September 2009.

Globalpark, Enterprise Feedback Suite, *EFS Conjoint Extension*, Version 1.7, Date 18.09.2008.

Green P.E., Krieger A.M., Agarwal M.K. "Adaptive Conjoint Analysis: Some Caveats and Suggestions", *Journal of Marketing Research* (28:2), 1991, pp. 215-222.

Green, P.E. and Srinivasan, V. "Conjoint Analysis in Consumer Research: Issues and Outlook", in *Journal of Consumer Research: An Interdisciplinary Quarterly* (5:2), University of Chicago Press, 1978, pp. 103-123.

Green, P.E. and Krieger, A.M. "Segmenting Markets with Conjoint Analysis", *Journal of Marketing* (55), 1991, pp. 20–31.

Green, P.E. and Srinivasan, V. "Conjoint Analysis in Consumer Marketing: New Developments with Implications for Research and Practice", *Journal of Marketing* (54), 1990, pp. 3–19.

Hair, J.F., Anderson, R.E., Tatham, R.L., Black, W.C. *Multivariate Data Analysis with Readings*, Prentice Hill, New Jersey, 1995, pp. 565.

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

Hann, I-H., Hui, K-L., Lee, T.S., Png, I. "Online Information Privacy: Measuring the Cost-Benefit Trade-off", in *Proceedings of the 23rd ICIS*, Barcelona, 2002. http://aisel.aisnet.org/icis2002/1. Accessed 30th April 2009.

Harper, J. and Singleton, S. "With a Grain of Salt: What Consumer Privacy Surveys Don't Tell Us", *Competitive Enterprise Institute,* 2001. DOI: 10.2139/ssrn.299930.

Harris Interactive "Most People Are "Privacy Pragmatists" Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits", 2003. http://www.harrisinteractive.com/harris_poll/index.asp?PID=365. Accessed 30th April 2009.

Hogben, G. (Ed.) "Security Issues and Recommendations for Online Social Networks", *ENISA Position Paper* (1) 2007. http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf. Accessed 30th April 2009.

Hui, K-L., Tan, B.C.Y., Goh, C-Y. "Online Information Disclosure: Motivators and Measurements", *ACM Transactions on Internet Technology* (6:4), 2006, pp. 415-441.

insidefacebook.com (2009) "Fastest Growing Demographic on Facebook: Women Over 55", 2009. http://www.insidefacebook.com/2009/02/02/fastest-growing-demographic-on-facebook-women-over-55. Accessed 3rd September 2009.

Jarvenpaa, S. L. and Tractinsky, N. "Consumer Trust in an Internet Store: A Cross-Cultural Validation", *Journal of Computer-Mediated Communication* (5:2), 1999. http://jcmc.indiana.edu/vol5/issue2/jarvenpaa.html. Accessed 3rd September 2009.

Jensen, C., Potts, C., Jensen, C. "Privacy Practices of Internet Users: Self-reports versus observed behavior", *International Journal Human-Computer Studies* (63:1-2), 2005, pp. 203-227.

Johnson R.M. "Trade-off Analysis of Consumer Values", *Journal of Marketing Research* (11:2), 1974, pp. 121-127.

Johnson, R.M. "Adaptive Conjoint Analysis", *Sawtooth Software Conference on Perceptual Mapping, Conjoint Analysis, and Computer Interviewing*. Sawtooth Software, Inc., Ketchum, ID, 1987, pp. 253-265.

Joinson, A. N., Paine, C., Buchanan, T., Reips, U.-D. "Watching me, watching you: Privacy attitudes and reactions to identity card implementation scenarios in the United Kingdom", *Journal of Information Science* (32:4), 2006, pp. 334-343.

Joinson, A. N. "Looking at, looking up or keeping up with people?: motives and use of facebook", *CHI '08: Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems,* ACM, New York, NY, USA, 2008, pp. 1027-1036.

Kolek, E. A. and Saunders, D. "Online disclosure: An empirical examination of undergraduate facebook profiles", *NASPA Journal* (45:1), 2008, pp. 1-25.

Krasnova, H. and Veltri, N. F., "Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA", in *Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS'10)*, 2010, accepted for publication, forthcoming.

Krasnova, H., Kolesnikova , E., Günther, O. "It Won't Happen To Me!": Self-Disclosure in Online Social Networks*", 15th Americas Conference on Information Systems*, San Francisco, 2009.

Lampe, C., Ellison, N., Steinfield, C. "A Familiar Face(book): Profile Elements as Signals in an Online Social Network", *SIGCHI conference on Human factors in computing systems*, San Jose, CA, USA, 2007, pp. 435-444.

Liehr, M. "Die Adoption von Kritische-Masse-Systemen: Das Problem der individuellen Kritischen Masse", Deutscher Universitäts-Verlag, Wiesbaden, 2005.

Lischka, K. „Riskante Strategie. StudiVZ setzt auf Schnüffel-Werbung", 2007. http://www.spiegel.de/netzwelt/web/0,1518,523286,00.html . Accessed 3rd September 2009.

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* (15:4), 2004, pp. 336-355.

McKnight, D. H., Choudhury, V., Kacmar, C. "Developing and Validating Trust Measures for E-commerce: An Integrative Typology", *Information Systems Research* (13:3), 2002, pp. 334-359.

Metzger, M. J. "Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce", *Journal of Computer-Mediated Communication* (9:4), 2004. http://jcmc.indiana.edu/vol9/issue4/metzger.html. Accessed 4th September 2009.

Orme, B. K. "Formulating Attributes and Levels in Conjoint Analysis", Research Paper Series, *Sawtooth Software*, 2002a.

Orme, B. K. "Interpreting conjoint analysis data", Research Paper Series, *Sawtooth Software*, 2002b.

Pavlou, P. A. "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model", *International Journal of Electronic Commerce* (7:3), 2003, pp. 101-134.

Phelps, J.E., D'Souza, G., Nowak, G.J. "Antecedents and consequences of consumer privacy concerns: an empirical investigation", *Journal of Interactive Marketing* (15:4), 2001, pp. 2-17.

Putman, R. D. "Bowling Alone: The Collapse and Revival of American Community", Simon & Schuster, New York, 2000.

Rizk, R., Marx, D., Schrepfer, M., Zimmermann, J., Günther, O. "Media Coverage of Online Social Network Privacy Issues in Germany - A Thematic Analysis", *15th Americas Conference on Information Systems*, San Francisco, 2009.

Sachoff, M. "Social Network Users Ignore Most Ads", 2008. http://www.webpronews.com/topnews/2008/11/26/social-network-users-ignore-most-ads. Accessed 30th April 2009.

Schonfeld, E. "Facebook Finances Leaked", 2008. http://www.techcrunch.com/2008/01/31/facebook-finances-leaked/ . Accessed 30th April 2009.

Schonfeld, E. “More Facebook Advertisers Bail From Beacon. Plus, New Concerns”, 2007. http://www.techcrunch.com/2007/12/03/more-facebook-advertisers-bail-from-beacon-plus-new-concerns/. Accessed 30th April 2009.

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

Smith, H. J., Milberg, S. J., Burke, S. J. “Information Privacy: Measuring Individuals’ Concerns About Organizational Practices”, *MIS Quarterly* (20:2), 1996, pp. 167-196.

Son, J.-Y. and Kim, S. S. “Internet Users’ Information Privacy-Protective Responses: A Taxonomy and a Nomological Model”, *MIS Quarterly* (32:3), 2008, pp. 503-529.

Srinivasan, V. “Surprising robustness of the self-explicated approach to customer preference structure measurement”, *Journal of Marketing Research* (34), 1997, pp. 286-291.

Strater, K. and Richter, H. “Examining Privacy and Disclosure in a Social Networking Community”, *Symposium on Usable Privacy and Security*, Pittsburgh, 2007.

StudiVZ “Daten und Fakten”, 2009a. http://www.studivz.net/l/about_us/1/. Accessed 7th Setember 2009.

StudiVZ “Über uns”, 2009b. http://www.studivz.net/l/press/. Accessed 7th September 2009.

Tufekci Z. “Can you see me now? Audience and disclosure regulation in Online Social Network Sites*”, Bulletin of Science, Technology & Society* (28:1), 2008a, pp. 20-36.

Tufekci, Z. "Gender, Social Capital And Social Network(ing) Sites: Women Bonding, Men Searching", *Annual Meeting of the American Sociological Association, Boston, MA,* 2008b. http://www.allacademic.com/meta/p242696_index.html. Accessed 7th September 2009.

Wolin, L.D. and Korgaonkar, P. “Web advertising: Gender differences in beliefs, attitudes and behavior”, *Internet Research* (13:5), 2003, pp. 375-385.

Xing “Benefits of Premium Membership”, 2009. https://www.xing.com/cgi-bin/user.fpl?op=benefit. Accessed 30th April 2009.