electronics

MDPI

Article

Avoiding the Privacy Paradox Using Preference-Based Segmentation: A Conjoint Analysis Approach

Marija Kuzmanovic * and Gordana Savic

Faculty of Organizational Sciences, University of Belgrade, Jove Ilića 154, 11000 Belgrade, Serbia; gordana.savic@fon.bg.ac.rs

* Correspondence: marija.kuzmanovic@fon.bg.ac.rs

Received: 15 July 2020; Accepted: 21 August 2020; Published: 27 August 2020

Abstract: Personal privacy on online social networks (OSN) is becoming increasingly important. The collection and misuse of personal information can affect people's behavior and can have a broader impact on civil society. The aim of this paper is to explore the privacy paradox phenomenon on OSNs that is reflected in the gap between OSN users' privacy concerns and behavior and to introduce a new segmentation framework based on preference data from conjoint analysis. For the purpose of the study, an online survey on four dimensions of OSNs has been conducted. Conjoint analysis has been employed on collected data to reveal users' preferences, followed by two-step cluster analysis for the preference-based segmentation. The characteristics of the resulting clusters were compared with self-reported behavior and privacy concerns, as well as the results of the Westin Privacy Segmentation approach. The results suggest that conjoint analysis can improve users' segmentation and consequently provide better solutions for avoiding the gap between users' concerns, attitudes, and behavior.

Keywords: online social networks; information disclosure; privacy paradox; behavior; conjoint analysis; preferences; preference-based segmentation; Westin privacy index

1. Introduction

Information privacy and data protection are major issues in today's digital society. Developed to simplify communication and information exchange and to enable various types of online entertainment and applications, online social networks (OSNs) are an especially vulnerable part of global information systems [1]. The expansion of OSNs has created a global communication phenomenon that has enabled billions of users to connect to others [2]. However, with the rapid growth of those networks and the number of their users, the number of threats and privacy issues also increases. Therefore, there are attempts [3] to provide a method for quantification of the privacy of individuals by measuring different aspects such as accessibility, reliability, privacy awareness, and visibility. The final goal is to help users to accurately recognize the state of their privacy and improve it.

Many studies have shown that OSN users' disclosure behavior does not align with their privacy concerns and that they are often conflicting [4]. Following these privacy issues, the privacy paradox phenomenon arises because individuals' stated intentions, attitudes, and preferences for disclosing information do not reflect their actual disclosure behavior [5,6].

According to Preibusch [7], privacy attitudes and privacy behavior are not always complementary and should be considered using specific procedures: behavior should be studied experimentally, while attitudes should be examined using surveys. A detailed review of 181 articles related to the privacy paradox [8] demonstrates that cognitive estimate and emotions are the most influential determinants of privacy-related behavior, while demographic characteristics are weak predictors. Different disciplines have employed different approaches to investigating the privacy paradox phenomenon; for example,

statistical approaches such as the multi-median approach [9], partial least square structural equation modeling [10], or explanatory factor analysis [11].

Providing a detailed review of studies related to the gap between the stated privacy concerns and actual online behavior, Barth and de Jong [12] conclude that the privacy paradox deserves far more research attention.

In this paper, we employ the conjoint analysis experimental procedure to measure OSN user preferences and investigate connections between their behavior, attitudes, and preferences related to the privacy. The motives for applying conjoint analysis were numerous. First, the assessment of hypothetical OSN profiles described by a set of factors is more realistic and similar to real situations in which respondents have to make trade-offs between conflicting factors. Second, OSN users' preferences are measured indirectly, which can reduce the bias of strategic responses. Third, preferences i.e., part-worth utilities are calculated for each individual respondent and can therefore be used for post hoc, so-called preference-based segmentation purpose. Furthermore, it is possible to compare the preferences of each respondent with their actual behavior and determine whether or not there is a privacy gap.

The separate part of the survey is designed to investigate the privacy concerns and habits of users. The main focus of the study is to generate a segmentation scheme based on user preferences. In the literature, the segmentation of users into groups of "fundamentalists", "pragmatists", and "unconcerned" according to the Westin privacy index [13] is the most common in Internet-based market research. However, results indicate a privacy gap between the predicted and actual behavior of users categorized to particular segments. On the other hand, the conjoint-based classification we propose in this paper generates more segments with a smaller gap between the predicted and actual behavior. The structure of this paper is as follows. Section 2 provides a literature review on privacy issues related to the OSNs. The third section gives an insight into the methodology and survey design used in the study, while the survey results are presented in Section 4. A detailed description of clusters identified on the basis of the preferences resulting from conjoint analysis follows in the second part of Section 4. Section 5 provides a comparative analysis of clusters isolated by applying the conjoint analysis and those categorized by the Westin approach. The sixth section, with the main findings, implications, limitations, and further direction of research concludes the study.

2. Literature Review

2.1. Online Social Networks and Privacy

OSNs are complex ecosystems that consist of a number of entities and stakeholders. Privacy and information security problems equally concern both service users and service providers regardless of their different roles in an OSN ecosystem. OSN providers are responsible for the proper handling of users' personal information, managing their activities and properly operating their own services while maintaining a profitable business model [14]. The privacy and security threats such as unauthorized sharing of personal information may disrupt proper functioning and damage providers' reputation [15]. Therefore, OSN providers invest effort to ensure the security of big data collections. Methods such as decentralization were considered as a solution to the privacy issues of OSNs, which resulted in a number of challenges and innovative technical solutions for their realization. An overview of decentralized privacy preserving social networking services is provided in Bahri, Carminati, and Ferrari [16].

However, OSN users interact with others using third-party social applications and click on ads placed by advertisers. All of these activities may lead to information leakage. A further security threat is an increased possibility of collecting personal data from multiple social networks and building a broader user profile. Park et al. [17] claim that dealing with these threats through OSNs is a crucial challenge to both service providers and OSN users. They suggest optimal data management as a tool to balance the benefits of using OSNs and privacy risks.

2.2. Privacy Paradox

The dichotomy between OSN user behavior and their attitudes has become a relevant research topic [18]. Even though recent research results show that information privacy is an important issue for OSN users [19], most of them rarely make sufficient effort in personal data protection [4,20]. This phenomenon is usually referred to in the literature as the privacy paradox. Although a real intention of data protection exists, common OSN user behavior goes beyond intentions in terms of personal data disclosure [21]. Several papers reviewed different theories introduced in online privacy information research. Li [22] considered privacy and risk issues and proposed a dual-calculus model for exploring trade-offs that influence the information disclosure behavior of individuals. The privacy calculus proposes the theory of trade-offs between an individual's intention to disclose information and possible benefits [23]. The risk calculus is based on the protection motivation theory [24] and calculates the trade-off between perceived risks and the efficiency of coping. The privacy paradox has been re-examined in the context of actual information disclosure over mobile devices based on individuals' realistic risk perceptions [5]. An attempt was also made to explore the website interactions of online shoppers and to resolve the privacy paradox based on cognitive and emotional aspects [10]. According to research, online consumers are more likely to disclose personal information when they have initial positive cognitive appraisals of a shopping website and if they like it. The intelligent prediction model, which uses interaction time and the topological structure of a user's relationship, has been developed to identify the diffusion critical paths and possibility of information leakage [25]. On the other hand, behavioral analysis has been employed to predict user attitudes toward unwanted content in ONSs [26].

Although there are real data protection intentions, the common behavior of OSN users goes beyond intentions for disclosing personal information. Barth and de Jong [12] examined 32 papers to investigate the correlation between the nature of users' decision-making process (in terms of rationality) and the privacy paradox. They claim that most users do not have the expertise or experience in appropriate protective behavior, especially when using mobile applications. Accordingly, a mix of rational and irrational decision making could explain the gap between privacy concerns and behavior, especially as it relates to mobile computing. A solution to the privacy paradox might lie in creating privacy awareness in combination with tools that help users avoid paradoxical behavior [27]. Hallam and Zanela made another theoretical attempt to explain the privacy paradox as a temporally discounted balance between concerns and rewards using a construal level theory lens [4]. Similarly, the study of 495 mobile social commerce users [9] tried to reveal the reasons behind the privacy paradox. The authors concluded that the privacy paradox phenomenon is caused by perceived mobility and social support, and that there is no correlation between users' concerns about the misuse of their data and their intention to use mobile devices.

Kokolakis [28] reviewed 18 papers that provide evidence to support the privacy paradox hypothesis and 12 papers that challenge it. He found that theoretical explanations for the privacy paradox usually stem from the privacy calculus theory, social theory, cognitive biases and decision-making heuristics, bounded rationality, decision making under information asymmetry, and quantum theory homomorphism. Gerber, Gerber, and Volkamer [8] extended the above-mentioned review by summarizing the theoretical and methodological aspects of the privacy paradox. Moreover, using structural equation modeling and regression analyses, authors attempted to explain it empirically. They found that information privacy concern was a good predictor of attitude toward online privacy, while general privacy concerns and user perception about controlling the processing of their data are crucial predictors of context-specific privacy concerns.

The results of a survey conducted in Sweden on 1703 respondents give an overall picture of how privacy concerns are perceived in different online contexts [29]. The findings have shown that although privacy concerns are highly dependent on the applications being used, trust in other people is undoubtedly the most important factor that explains privacy concerns.

Beak [30] used a counterargument experimental technique through three experiments in which 79, 279, and 71 students, respectively, were exposed to different messages. He found that the privacy paradox appeared in conventional polls but disappeared in counterargument conditions. Li et al. [10] used partial least square structural equation modeling on data collected in a survey of 152 students, and the results have shown that privacy concerns have a minimal effect on behavior in the presence of situation-specific cognitive appraisals and emotions. Using explanatory factor analysis, Choi et al. [11] have shown that a new aspect of privacy, fatigue, has a stronger impact on privacy behavior than privacy concerns. The univariate analyses of the impact of different activities on an OSN, such as posting types, content, and audiences, indicate that Facebook users are more concerned about other users posting on their own timeline, while on Twitter, they are more concerned about their own tweets than other users retweeting their tweets [31].

Lee and Kwon [32] deal with privacy issues in the context of personalization of mobile wellness healthcare services. They propose a privacy-aware feature selection method based on the privacy paradox that considers the personal characteristics of customers using these services.

3. Materials and Methods

We employed the technique of conjoint analysis to identify OSN user preferences toward privacy and to group them into adequate segments. The data were collected through a web-based questionnaire, which included four sections: (1) Conjoint analysis tasks (stimuli) from an efficient experimental design; (2) Socio-demographic questions, (3) Questions regarding respondents' habits in using OSNs, both general and privacy-related, and (4) Respondents' concerns toward data privacy and safety.

3.1. Conjoint Analysis Design

Conjoint analysis (CA) is a stated preference method that aims to experimentally uncover the hidden rules that individuals use to make trade-offs between products or services. Although it originated in mathematical psychology and was first used in marketing to determine consumer preferences, CA has found wide application to understand individual preferences in numerous areas and in different contexts [33–36].

When it comes to privacy issues, CA was used to investigate the importance of privacy-preserving techniques related to sharing personal health data in online health systems [37]. The results indicated that respondents were sensitive to sharing data for commercial purposes, especially in the case of mental illness, while they have shown little concern about sharing data for scientific purposes and sharing data related to physical illnesses. Krasnova et al. [38] used CA to examine the factors influencing the choice of an OSN and determined that price and social network popularity are crucial for making this decision.

In order to measure user preferences toward key dimensions of OSNs, including privacy, this study followed five key steps.

Step 1: Identification of key factors and factor levels. The first and most important step in CA is to identify the list of relevant factors (attributes) that could influence individual preferences. The list should include those factors that are both more relevant to the potential customer (OSN user) and that may be influenced or manipulated by the social network service provider. Then, each factor must be assigned performance levels that should be credible, effective, and that can be traded off against one another. This conjoint study evaluated individual trade-offs among the four OSN factors, two of which are related to privacy concerns (see Table 1). To identify other factors, we used literature review and interviews.

Existing OSNs differ in their popularity among users; some of them are widespread with a large number of members (such as Facebook), others are smaller or specialized (such is LinkedIn). This study assigns three levels to the given factor, depending on the frequency of use among the respondents' acquaintances. Levels are expressed as percentages of acquaintances who are users of that particular network, i.e., 25%, 50%, or 75%.

Table 1. Factors and factor levels used in survey. OSN: online social networks.

Dimension	Factor	Level	Code
I Popularity	OSN popularity among acquaintances	25%	N1
		50%	N2
		75%	N3
II Customizability	Possibility to customize OSN environment	Yes	C1
		No	C2
III Privacy	Privacy Control options given to users	All or friends	O1
		Predefined groups	O2
		Particular friend	O3
	Information used by OSN provider	No information	P1
		Demographic	P2
		All information	P3

OSNs can vary in the extent of individual profile customizability, which allows users to represent themselves in a desired way. In this study, we list two levels related to this factor: Without Customizability (OSN does not offer the ability to distinguish their own profile from others) or With Customizability (OSN allows users to customize their profile to a certain extent in terms of appearance and applications).

OSNs may vary in the degree of privacy control options available to users. This option allows users to define who can access their information. In our study, three levels are listed for this factor. The first level implies that a user can allow the profile to be available for access either to all OSN users or just to friends (All or Friends). Users can also organize friends into groups and specify which parts of the profile different groups can access (Predefined Groups), or they can specify which parts are accessible to a particular friend (Particular Friend).

Network maintenance always costs a service provider. Accordingly, the OSN provider sometimes uses the information collected from users to provide personalized advertising. In general, the information may belong to two groups: demographic and personal. Thus, in this study we specify three levels for the factor Information used by an OSN provider: "No information is used", "Only demographics is used", and "All info is used".

Step 2: Experimental design construction. By combining the above-mentioned four factors and their levels, a total of 54 ($3^3 \times 2$) conjoint stimuli (hypothetical OSNs) can be made. To reduce this number of stimuli to a manageable set of 9, statistical package SPSS 20.0 was used, and more specifically the Orthoplan component. This component generates a fractional factorial design known as orthogonal array, in order to capture the main effects of each factor level. For example, one particular stimulus was an OSN with 50% popularity, where users can customize their profile to distinguish from others, organize friends into groups, and specify which parts of the profile are visible to different groups, while the OSN provider may collect and use only the user demographic data.

Step 3: Choosing a presentation method. Prior to the part of the survey related to the conjoint analysis tasks, individuals were asked to imagine that they need to select an OSN that best suits their preferences. They were asked to evaluate each of the 9 stimuli on the Likert scale ranging from 1 ('least preferred') to 5 ('most preferred').

Step 4: Model specification and estimation technique selection. After collecting information about individual preferences, it is necessary to analyze the responses and perform parameter estimation. In this study, the linear additive model of part-worth utilities is employed. This model assumes that the overall OSN evaluation consists of the sum of contributions of the factor levels [39]. The model comprises four factors (k = 1,...,4), each one with L_k levels, and states as follows:

$$\begin{aligned} U_{ij} &= \sum_{k=1}^{4} \sum_{l=1}^{L_k} \beta_{ikl} x_{jkl} + \varepsilon_{ij} = \beta_{iN1} x_{jN1} + \beta_{iN2} x_{jN2} + \beta_{iN3} x_{jN3} + \beta_{iC1} x_{jC1} + \beta_{iC2} x_{jC2} + \\ &+ \beta_{iO1} x_{jO1} + \beta_{iO2} x_{jO2} + \beta_{iO3} x_{jO3} + \beta_{iP1} x_{jP1} + \beta_{iP2} x_{jP2} + \beta_{iP3} x_{jP3} + \varepsilon_{ij}, \quad i = 1, \ldots, I, \;\; j = 1, \ldots, J \end{aligned} \tag{1}$$

where U_{ij} is a dependent variable representing the evaluation of stimuli j by respondent i; while x_{jkl} is the binary variable, indicating the presence ($x_{jkl} = 1$) or absence ($x_{jkl} = 0$) of the lth level of the kth factor in the stimuli j. Coefficient β_{ikl} is individual i's utility associated to the level l of the factor k (part-worth), while ε_{ij} is a stochastic error. Since each stimulus may include only one level of each factor, the constraint (2) must be fulfilled:

$$\sum_{l=1}^{L_k} x_{jkl} = 1, \qquad j = 1, \ldots, J, \; k = 1, \ldots, K. \tag{2}$$

Individual part-worth utilities are estimated using least-squares regression, providing a quantitative measure of the preference for each factor level, with higher values corresponding to a higher preference. The total utility, i.e., the overall preference for any combination of factor levels can be determined by adding the estimated part-worths of appropriate factor levels. Partial utilities are also used to determine the relative importance of factors that are calculated as the ratio of the utility range of the given factor to the total utility range of all factors:

$$FI_{ik} = \frac{\max\limits_{l}\beta_{ikl} - \min\limits_{l}\beta_{ikl}}{\sum\limits_{k=1}^{K}\left(\max\limits_{l}\beta_{ikl} - \min\limits_{l}\beta_{ikl}\right)}. \tag{3}$$

The factors' importance can further be calculated for a particular group of individuals or for the whole sample.

Step 5: Segmentation (Clustering). Cluster analysis has been applied to determine whether individuals consistently differ in the compromises they would make between the benefits of OSN popularity, the option to customize an OSN environment, and privacy concerns. By applying this technique, subjects can be grouped into distinct segments according to the similarity of utilities estimated for various factors. Both the part-worth utilities and the resulting relative importance values can be used for preference-based segmentation. In this study, we used the two-step cluster analysis to segment individuals according to the estimated factor importance scores.

3.2. Privacy-Related Survey Design

In addition to the conjoint tasks, the survey included three other sections. Section 2 comprises the socio-demographic questions regarding gender, age, level of education, employment status, and marital status. Section 3 contains questions related to respondents' habits in using OSNs, as well as questions related to behavior with regard to their own and their friend's privacy. Some of them are:

- Purpose of using OSNs and their primary choice of OSN;
- Frequency of activities such as establishing new friendships, chatting, general information sharing, finding information about social events, etc. on OSNs;
- Intentions of sharing personal data (real name, profile picture, e-mail, phone number, date of birth, place of residence, relationship status) within OSNs; users are usually more concerned about their privacy compared to other online situations. Therefore, content sharing is one of the key features in OSNs.
- Privacy-related behavior.

Section 4 includes questions regarding privacy concerns with OSN use as well as previous experience with invasion of privacy. This section also comprises three statements from the Westin Privacy Segmentation Index (WPSI) [13]. The statements, adapted to the subject of this research, are as follows:

Q1. *OSN users have lost all control over how personal information is collected and used by online social network providers.*

Q2. *Most OSN providers treat the personal information they collect about OSN users in a proper and confidential manner.*

Q3. *Existing laws and organizational practices provide a reasonable level of OSN users' privacy protection today.*

The WPSI has been widely used as an instrument to measure privacy attitudes and categorize individuals into three privacy segments: fundamentalists, pragmatists, and unconcerned [13,40,41]. Privacy fundamentalists are individualists that are the most protective when it comes to their privacy. According to Krane et al. [40], these individuals "feel companies should not be able to acquire personal information for their organizational needs and think that individuals should be proactive in refusing to provide information". The opposite to fundamentalists, privacy unconcerned individuals are very comfortable with sharing data and believe that such behavior does not threaten their privacy. Between these two extremes are the so-called privacy pragmatists. Before they decide to share their personal information, pragmatists evaluate the risks of releasing personal information against the potential benefits. WPSI is used as a reference point for the comparison of the results obtained through the approach we propose in this paper, which is based on the preferences derived from conjoint analysis.

4. Results

In accordance with the aim of the research, respondents were recruited through convenience sampling and purposive sampling methods. The survey was shared via Facebook, LinkedIn, Instagram, and other social networks. The intention was to reach OSN users who would be willing to provide the most relevant data to answer the defined research questions.

A total of 938 individuals responded to the survey. After eliminating incomplete and inconsistent surveys, 843 eligible surveys were used in further analysis. Just over two-thirds of the respondents (71.4%) were women. The average age was 25.9 (SD = 8.511), with the highest percentage ranging from 20 to 25 years (54.6%). The majority of respondents completed high school (41.4%) or gained one of the university degrees (54.4% in total). One-quarter of respondents were employed (25%). Almost half of the sample (49.5%) consisted of respondents who were single in terms of relationship status, and only 13.6% were married. The detailed demographic data are given in Table 2.

4.1. Respondents' Behavior in Using OSNs

We investigated respondents' behavior in using OSNs, both general and privacy related. The results indicate that an almost equal number of respondents use OSNs exclusively for private (49.6%) and for private and business purposes (49.4%), while a negligible number of them use it solely for business purposes (only 1.1%). Most respondents listed Facebook as their first choice (70.2%), followed by Instagram (10.8%), WhatsApp (9.5%), and Viber (6.4%), while other OSNs took only 3.1%.

As can be seen from Figure 1, respondents most often use OSNs to exchange information, chat, and find information about social events, rather than to establish new acquaintances, and only 3.08% of respondents often do so.

A more detailed analysis of the responses showed that the majority of married respondents (75.7%) and 58.8% of the respondents who are in a relationship have never used an OSN for making new relationships. On the other hand, 53.2% of the single respondents have used an OSN for that purpose. When it comes to chatting, only 2.4% of the singles claim that they are not chatters, while the percentage of those who are married and are not chatters is 15.7%. All high school students (100%) and most of the university students (96.9%) chat, while 10.7% of the employed never chat (10.7%).

Table 2. Demographic data.

Demographic	Category	Number	Percent
Gender	Male (M)	241	28.59%
	Female (F)	602	71.41%
Age	16–19	128	15.18%
	20–25	460	54.57%
	26–35	129	15.30%
	36–45	95	11.27%
	>45	31	3.68%
Level of education	Primary school	38	4.51%
	High school	349	41.40%
	Undergraduate	292	34.64%
	Master degree	147	17.44%
	PhD degree	17	2.02%
Employment status	Students (high school)	56	6.64%
	Students (university)	488	57.89%
	Unemployed	54	6.41%
	Employed	243	28.83%
	Retired	2	0.24%
Relationship status	Single	417	49.47%
	In relationship	311	36.89%
	Married	115	13.64%

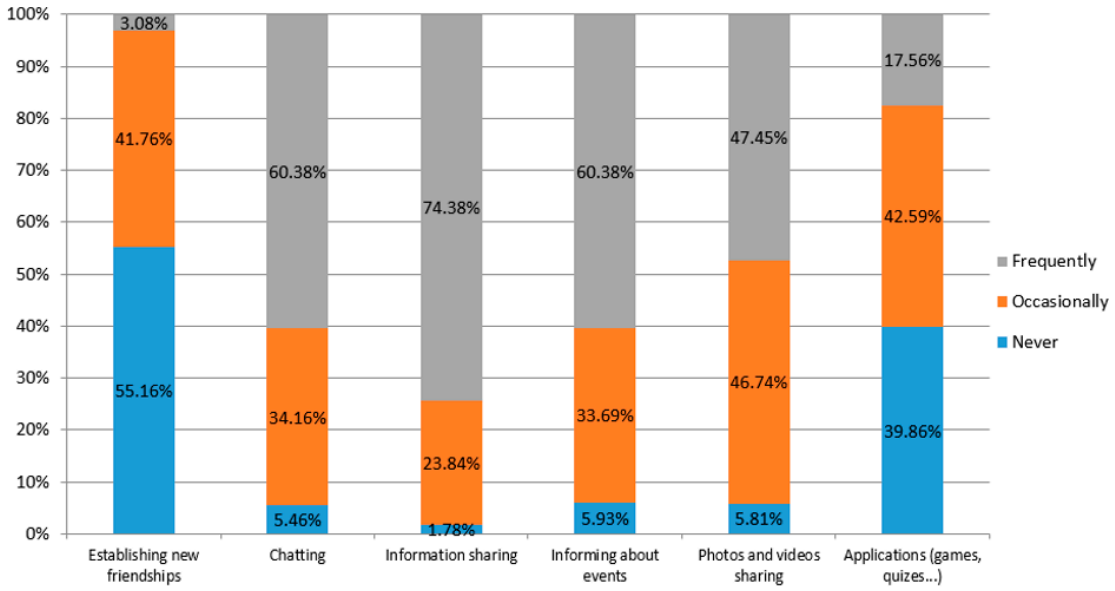

Figure 1. Frequency of online social networks (OSN) activities.

The first set of questions regarding actual privacy behavior was related to the public placement and online availability of personal data and materials. For the majority of items, respondents answered that it depends on the OSN. The detailed results are shown in Figure 2.

As for sharing intentions, the majority of the respondents share personal data, photos, videos, and posts with all friends, and a significantly lower percentage of respondents share with all OSN users.

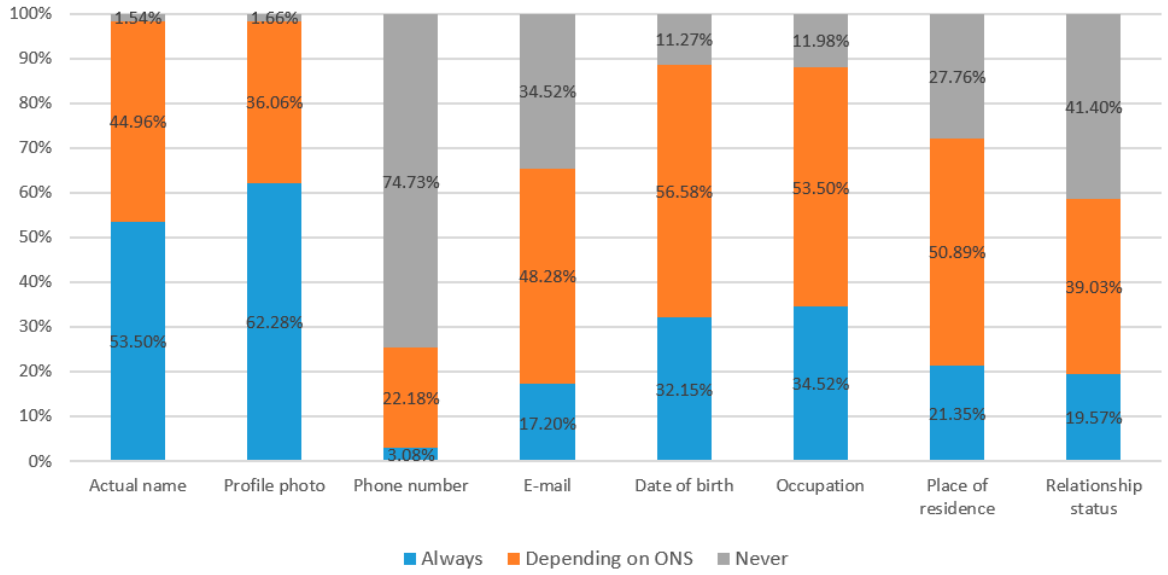

Figure 2. Personal data sharing.

When it comes to privacy and safety behavior, respondents have shown a high level of responsibility for certain issues. Namely, almost two-thirds of the respondents never accept friend requests from unknown persons and do not access their own profile from public computers (see Figure 3). However, over 50% of the respondents are being checked-in during visits to some places, and as many as 60% of them occasionally access applications that try to collect data.

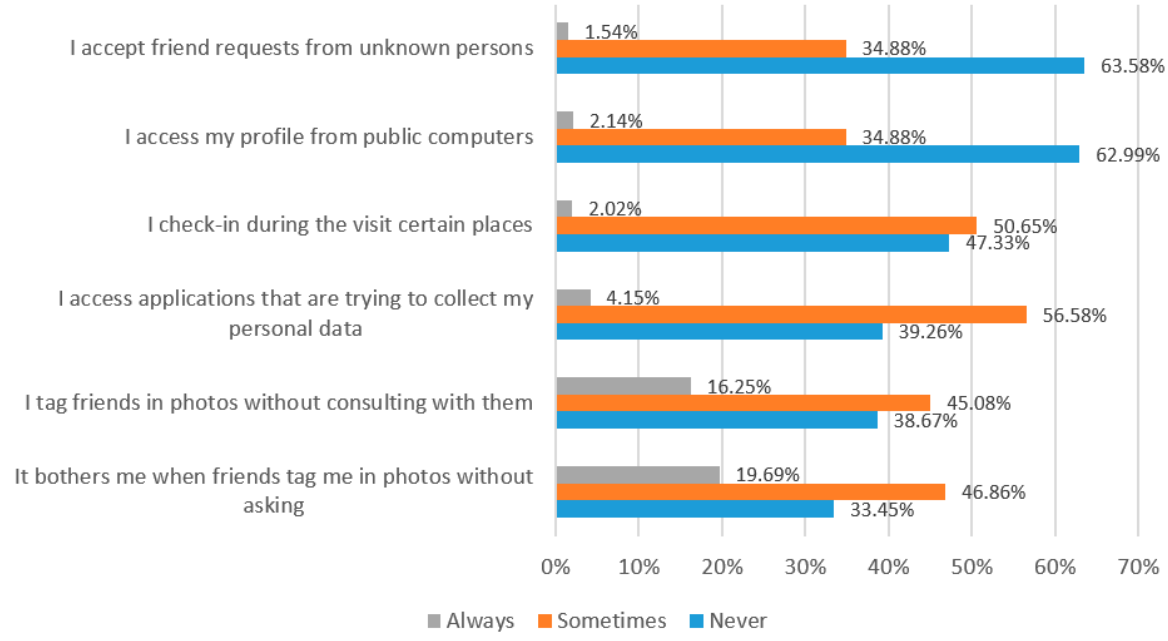

Figure 3. Privacy-related behavior.

4.2. Respondents' Concerns for Data Privacy and Safety

Most respondents showed moderate concern about the privacy of personal data and photos (mean score 3.05, SD = 1.145), with 13.8% of those showing extreme concern. They are somewhat less concerned about the privacy of their friends' data and photos (mean score 2.60, SD = 1.050), and just 4.7% of them are extremely concerned. In addition, we have explored the respondents' experience

with abuse and violation of privacy on OSNs. A small percentage of respondents (8.7%) state that they have had such an experience, while 45.4% claim that they have never had such an experience. The remaining 42.9% respondents are not sure.

The results obtained by applying the Westin Privacy Segmentation Index instrument show that 52.19% of the respondents are pragmatists (55.15% female, 44.81% male), 43.65% are fundamentalists (40.53% female, 51.45% male), and 4.15% are unconcerned (4.32% female, 3.73% male). Using the chi-square test, we examined whether belonging to a particular Westin segment is associated to members' demographics. It was found that young respondents aged 16 to 19 are mostly pragmatists (59.4%) and as many as 7.8% of them are unconcerned. Respondents aged 20–25 are also mostly pragmatic 57.8%, but only 3.5% of them are unconcerned, while those over 25 are mostly fundamentalists (56.8%) ($p = 0.000$). Moreover, 54.2% of singles and 53.4% of those in a relationship are pragmatists, while the majority of those who are married are fundamentalists (55.7%). These results are statistically significant at $p < 0.1$.

We further examined whether the behavior in using OSNs is in line with the predicted Westin categories. A statistically significant difference occurred in the intentions to share some personal data (real photo and date of birth), as well as the accessibility to personal information and posts. When it comes to accessing their profile from public computers and accepting an unknown friend request, statistically significant differences were not found between the identified segments. Moreover, when it comes to accessing applications that collect information, the results are contradictory: a smaller percentage of all fundamentalists (35.3%) than pragmatists (42.3%) and unconcerned (42.9%) never do this, which is in contrast to the expected behavior of a fundamentalist.

4.3. Aggregated Respondents' Preferences

Using conjoint procedure in SPSS 20.0, the parameters are estimated both for each respondent in the sample and for the sample as a whole. Table 3 shows the aggregated part-worth utilities for each factor level and the relative importance scores for all factors. Part-worth utilities reflect the attractiveness of factor levels, while the relative importance of a factor allows us to draw conclusions about the role that the factor has in users' decisions about OSN selection. Higher part-worth utility values indicate a greater preference.

Table 3. Aggregated customer preferences.

Factor	Level	Utility Estimate	Std. Error	Importance Scores
OSN popularity	25%	−0.639	0.035	32.61%
	50%	0.200	0.035	
	75%	0.438	0.035	
OSN environment customizability acoording own preferences	Yes	0.029	0.026	10.51%
	No	−0.029	0.026	
Privacy control by User	All/Friends only	−0.370	0.035	25.15%
	Predefined groups	−0.037	0.035	
	Particular friend	0.407	0.035	
Information used by OSN provider	No information used	0.466	0.035	31.73%
	Demography only	0.173	0.035	
	All information	−0.639	0.035	
(Constant)	-	2.729	0.026	-

The internal consistency of the model was measured in three ways. The predictive validity of the model is estimated by Kendall's Tau statistic. The value of 0.999 indicates that there is a strong correlation between the observed preferences and those estimated by the model, indicating the high predictive validity of the model. A high Pearson coefficient value of 0.889 confirms a high level of significance of the obtained results. Signs of all regression coefficients were as expected. For example, all other characteristics remaining the same, the respondents would prefer the most popular OSNs.

The conjoint data given in Table 3 indicate that the most important factor on the aggregate level is OSN Popularity, with an importance value of 32.61%. As expected, the total utility of OSNs increases with the increase of an OSN's popularity, but a change from the 25% to 50% level is more valuable than a change from 50% to 75%. Slightly less important is the factor Information used by OSN provider, with a relative importance of 31.73%. It can be noted that the total utility is higher when less information is collected about the user. However, the change from Demography only to All information more significantly reduces total utility than when it comes to changing from No information is used to Demography only. This is consistent with the findings in [38] and [42].

Privacy Control by User is the third most important factor (25.15%), whereas users prefer to have the possibility of greater control. This is in line with some other findings that show that "the need for customers to control their personal information is an important factor in reducing privacy concerns" [38,43]. The least important factor is Customizability with an importance value of just 10.51%.

The value of the constants given in Table 3 represents the stochastic error of the regression model (1) and is used to calculate the total utility of each stimulus.

Looking at the highest part-worths for each factor, an ideal OSN from the users' perspective can be derived: the OSN should be very popular among acquaintances (to include at least 75% of them), the provider does not use any private information, the OSN allows control over accessibility for a particular friend or groups of friends, and customizability is possible. The overall utility of such an OSN is 4.069 ($U = 0.438 + 0.029 + 0.407 + 0.466 + 2.729$). However, in case the OSN provider could use demographic data, the preferences would be reduced by about 7.20% ($U = 3.776$); if the OSN provider could use all data, the preferences would fall by as much as 27.16% ($U = 3.776$). Such an analysis is possible for all the potential factor combinations or level changes.

4.4. Cluster Analysis

A two-step cluster analysis based on the relative factors importance was employed in order to determine groups of OSN users with similar preferences. As a result, five clusters were identified. Table 4 shows the relative factor importance for each cluster, as well as part-worth values of the factor levels across clusters.

We further used the chi square to investigate whether cluster membership was systematically dependent on certain socio-demographic variables or respondents' privacy-related behavior and concerns. It is noted that there is a statistically significant difference in the following socio-demographic factors: gender ($p = 0.024$), education ($p = 0.007$), occupation ($p = 0.000$), age ($p = 0.007$), and events ($p = 0.016$). Detailed data are provided in Table A1 in Appendix A. When it comes to behavior and concerns related to privacy and safety, a statistically significant difference was noted in sharing intentions and privacy-related behavior, as well as in privacy and safety awareness (for details, see Table A2 in Appendix A).

4.4.1. Cluster 1: Fundamentalists

For this largest cluster, comprising 33.45% of respondents, the most important factor is privacy in terms of the possibility of their data being used by service providers (47.68%), followed by OSN popularity (24.56%). The overall importance of privacy-related factors is at a high level of 67.85%. According to its description, this cluster most closely corresponds to the Westin segment of Fundamentalists.

The members of this cluster are much less sensitive to the change in the popularity of an OSN from 75% to 50%, but they are much sensitive to the change from 50% to 25% (see Figure 4). The largest percentage of respondents who mainly use LinkedIn and Twitter belong to this cluster. The ratio of men and women in this cluster is proportional to their ratio in the entire sample. There are also similar holds for the age, but there are slightly more individuals aged 26–35.

Table 4. Relative factor importance and part-worth utilities across clusters.

Factor	Level	Cluster 1 n = 282 (33.45%)	Cluster 2 n = 204 (24.20%)	Cluster 3 n = 151 (17.91%)	Cluster 4 n = 184 (21.83%)	Cluster 5 n = 22 (2.61%)
				Part-Worth Utilities		
OSN popularity	25%	−0.558	−0.548	−0.372	−1.011	−1.237
	50%	0.245	0.202	0.077	0.248	0.066
	75%	0.313	0.346	0.295	0.763	1.172
Customizability	Yes	0.030	−0.011	0.093	0.026	−0.015
	No	−0.030	0.011	−0.093	−0.026	0.015
Privacy control by user	All/Friends only	−0.331	−0.651	−0.286	−0.232	0.005
	Predefined groups	−0.031	−0.069	−0.038	−0.016	0.005
	Particular friend	0.362	0.720	0.324	0.248	−0.010
Information used by OSN provider	No information used	0.794	0.365	0.260	0.295	0.035
	Demography only	0.285	0.142	0.057	0.154	−0.025
	All information	−1.079	−0.507	−0.316	−0.449	−0.010
				Relative Factor Importance		
OSN popularity		24.56%	27.36%	24.76%	49.86%	94.06%
Customizability		7.59%	6.63%	23.59%	9.68%	1.14%
Privacy control by user		20.17%	40.06%	26.40%	17.97%	1.95%
Information used by OSN provider		47.68%	25.95%	25.25%	22.49%	2.86%
Privacy Total		67.85%	66.01%	51.65%	40.46%	4.81%

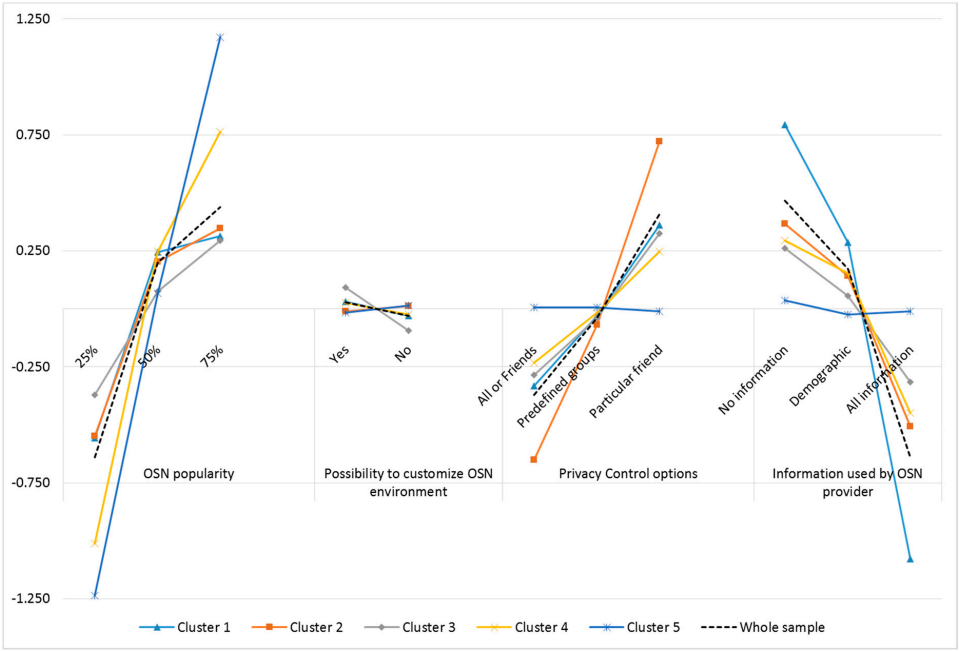

Figure 4. Part-worths functions across clusters.

They use the option that either only selected or all friends have access to their personal information, photos, and posts, and avoid accessing their own profile from a public computer more often than members of other clusters. The same applies to accepting a request for friendship from unknown persons. They also care about being tagged by friends without their permission much more than other clusters. They usually avoid accessing applications that can collect data; as many as 42.91% never do it.

When it comes to concern for personal data, as many as 36.4% state that they are very concerned and take care, while only 8.87% state that they are absolutely not concerned (the average score is 3.24, which is well above the average of 3.05 at the sample level). When it comes to the information about friends, cluster members show much less concern, which also holds for the sample as a whole. Nevertheless, as many as 18.3% of them are very concerned, and the average score for this criterion of 2.72 is higher than those for the sample.

In case a service required payment, 41.5% of cluster members would not use the given OSN, and only 11.35% would use the same as before, regardless of the payment.

4.4.2. Cluster 2: Pragmatists Tending to Privacy Control

As can be seen in Table 3, the overall importance of privacy-related factors for Cluster 2 is also at a high level (66.01%). However, the most important factor for members of this cluster is whether they can independently adjust privacy settings (40.06%). The OSN popularity in this second-largest segment (24.2% of sample) is also very important in terms of whether a provider can use their data (25.95%). The members' preferences fall almost linearly with the reduction in the possibilities of personal control of their own privacy (Figure 4).

The possibility to customize the OSN environment has very little importance, only 6.63%. The members of Cluster 2 especially prefer the possibility of setting permission individually for each person on an OSN, which is in accordance with their preferences.

Cluster 2 is mostly made up of young people aged 20–25 who most often use OSNs to find information about social events. The largest percentage of women and students is in this cluster. Access to personal information is usually allowed only to friends or particular friends, while access to photos and posts is usually allowed to particular friends. Cluster 2 does not accept requests for friendship from strangers to a greater extent than all other clusters.

When it comes to concern for personal data, as many as 29.91% state that they are very concerned—however, to a much lesser extent than in Cluster 1. On the other hand, as with Cluster 1, only 9.31% state that they are absolutely not concerned. The situation is similar when it comes to their concern about friends' information. The average grades are 3.10 and 2.71 respectively, which is more than the sample average. In case they should pay for using an OSN, the majority of cluster members (48.5%) would choose some OSNs, and only 13.2% would use all the same features as before.

4.4.3. Cluster 3: Pragmatists

The percentage of respondents belonging to Cluster 3 is 17.91%. This cluster is characterized by the balanced importance of all factors. It is also the only cluster that emphasizes the importance of having the possibility to customize an OSN environment (Figure 4). Privacy-related criteria take 51.65% of the total importance.

A slightly higher number of women and almost half of all high school students (46.43%) are in this cluster. Cluster members mostly allow access to personal data and photos to friends and friends of friends, while the majority of this cluster allows access to their posts to everyone. They access their profile from public computers and accept friendship requests from unknown persons much more often than the first two clusters.

They disapprove of being tagged without permission (as Clusters 1 and 2), but they are less concerned about the personal information (2.95) as well as the information about friends (2.62). In case they should have to pay, as many as 47.7% of them would no longer use the particular OSN, whereas 17.9% would decide to use all the same features as before, regardless of the payment.

4.4.4. Cluster 4: Socially Oriented Pragmatists

The fourth cluster is medium in size (21.83%) and includes respondents who are basically pragmatic but also socially oriented. The importance of privacy-related factors is much lower than in Clusters 1 and 2 (40.46% in total). The most important factor is OSN popularity (49.86%), followed by whether the OSN provider is allowed to use their data and to what extent (22.44%).

Most of the students, aged 20 to 25, are in this cluster. To a significantly higher extent than the previous three clusters, they choose the option to allow everyone on the OSN access to their personal data, while access to photos and posts is usually allowed to friends or friends of friends. In addition, they access their profile from public computers more often than the previous three clusters, and they accept requests for friendship from unknown persons much more often than Clusters 1 and 2. When it comes to accessing applications that try to collect personal data, they behave similarly to Clusters 1 and 2, i.e., they are more careful than the third and fifth cluster, which is in line with

their preferences. Finally, they are less concerned about personal data (2.90) and information about friends (2.44).

4.4.5. Cluster 5: Unconcerned

Although this is the smallest segment (2.61% of the total sample), it is distinguished for its specific characteristics. Much of the cluster is made up of men aged 26–35. The most important criterion for members of this cluster is network popularity (as many as 94.06%), while the privacy is negligibly important for them (4.81% in total). They disregard privacy control (1.95%) and are unconcerned about what information will be taken by the OSN provider (2.86%).

Members of this cluster use OSNs considerably more to find information about events; 86.36% use them often, while the other 13.64% use them occasionally. Around 60% of the cluster members access their profile from public computers, which is well above the sample average of 37%.

Compared to only 1.54% of sample respondents who always accept friend requests from strangers, as many as 13% of this segment always doe. They did not rate concerns about the data on friends with grades 4 and 5 (average score is only 1.55), and the concern for personal data is also at a very low level (2.05). As many as 41% of them would still use the same OSNs in case they had to pay (compared to the sample average of 15.18%). The behavior of this cluster is definitely in line with their preferences.

5. Comparison of WPSI and CA Clusters

Table 5 provides a comparative analysis of clusters isolated by applying the conjoint analysis and those categorized by the Westin approach. The percentages of members of a certain Westin category in each of the CA clusters are given in the brackets. Although the largest percentage of Westin fundamentalists is in Cluster 1 (CA fundamentalists), a large percentage is also found in the next three clusters. A high percentage of Westin pragmatists is also in CA Cluster 1, as well as CA Clusters 2 and 4. However, the percentage of Westin pragmatists is slightly lower in CA Cluster 3 (CA pragmatists). Westin Privacy unconcerned individuals are mostly in the first cluster, i.e., in CA fundamentalists. It can be noted that only one respondent is classified as Unconcerned according to both approaches.

Obviously, the results of the two approaches do not match to a great extent. The question is which of them better reflects the real state, i.e., which one is in line with the actual behavior of the respondents.

The results of the two approaches gave rise to a great contradiction. Namely, 11 (9 female and 2 male respondents) unconcerned according to WPSI were classified as fundamentalists according to CA, and 10 (4 female and 6 male respondents) fundamentalists according to WPSI were classified as unconcerned by CA. Therefore, these respondents are of particular interest for further analysis.

Table 5. Conjoint analysis (CA) vs. Westin Privacy Segmentation Index (WPSI) clusters.

CA \ WPSI	Privacy Fundamentalists	Pragmatists	Privacy Unconcerned	Total
Fundamentalists	143 (38.86%)	128 (29.09%)	11 (31.43%)	282 (33.5%)
Pragmatists tending to privacy control	80 (21.74%)	116 (26.36%)	8 (22.86%)	204 (24.2%)
Pragmatists	62 (16.85%)	80 (18.18%)	9 (25.71%)	151 (17.9%)
Socially oriented pragmatists	73 (19.84%)	105 (23.86%)	6 (17.14%)	184 (21.8%)
Unconcerned	10 (2.72%)	11 (2.50%)	1 (2.86%)	22 (2.6%)
Total	368 (43.7%)	440 (52.2%)	35 (4.2%)	843

A detailed analysis of the behavior of the first group of 11 respondents resulted in the following findings:

- 54.55% of individuals never access applications that try to collect data (the sample average is 39.6%), while others do it occasionally, and none of them do it always;

- As many as 72.73% individuals do not access their profile from public computers (the average is 62.99%);
- 63.64% do not accept friendship requests from unknown persons;
- More than half of the group allows access to personal data only to certain friends (the sample average is 28.35%);
- None of these respondents allow access to photos online, and 36.36% allow access only to particular friends (the average is 24.67%);
- No one had any experience with abuse and violation of privacy on OSNs;
- No one would continue to use the same OSNs in case they needed to pay (most would choose some of them);
- When it comes to concern for personal and friend data, average scores are 2.91 and 2.36, respectively.

Based on the above-mentioned data, it can be concluded that these 11 respondents are very protective of their privacy, which certainly corresponds more to privacy fundamentalists than to privacy unconcerned.

The second group of respondents showed the opposite privacy-related behavior:

- 10% always and 50% occasionally access applications that try to collect data;
- Significantly lower percentages never access their profile from public computers (40% compared to an average of 62.99%);
- 50% of these respondents accept friendship requests from unknown persons occasionally or always;
- As many as 30% allow access to their personal data to everyone on the OSN (sample average is 9.73%);
- As many as 50% would continue to use all OSNs in case they needed to pay;
- They show much less concern for both personal data and information about friends. Average scores for these criteria are 2.2 and 1.7.

Based on the above-mentioned data, it can be concluded that these 10 respondents are less protective of their privacy, which corresponds more to privacy unconcerned than to privacy fundamentalists.

The analysis indicates that the behavior of members of certain clusters in terms of privacy on the OSNs is in accordance with their preferences. Furthermore, for segments identified by CA, there is no gap between behavior and preference (as with Westin segmentation), which indicates that CA can be successfully used for the purpose of clustering indexing and even for predicting the behavior of OSN users when it comes to privacy.

6. Discussions and Conclusions

The aim of this paper was to research the privacy paradox phenomenon on OSNs, which is reflected in the gap between OSN user attitude and behavior, and to introduce a new segmentation framework based on preference data from the conjoint analysis.

The privacy paradox is becoming a relevant research subject, since it is proven that even though the majority of OSN users state that they are concerned about their data privacy, the majority of them rarely take proper care of personal data protection. Much research has been done on privacy issues on OSN, but most of these studies have addressed the factors that influence information disclosure and the influence of socio-demographic variables on a particular type of behavior [10,18,19,22,23,25]. Moreover, studies dealing with the clustering of OSN users based on privacy-related preferences, intentions, and behavior are rare. Explicitly, privacy calculus theory deals with identifying trade-offs between the expected costs and benefits of information disclosure, with these benefits and costs depending on the individual weighting of their components [22,23]. In order to investigate the importance of factors in predicting online behavior, different quantitative methods such as the multi-median approach [9], partial least square structural equation modeling [10], or explanatory factor analysis [9–11] have been used. Those methods mainly work with experimentally conducted data

or data collected through surveys containing self-explicated questions. Some of them calculate only aggregated results, consider intentions and not current behavior, and do not consider heterogeneity in preferences but rather socio-demographic data. Having in mind that deciding to provide personal information online is a complex psychological process [8], conjoint analysis appeared to be an adequate method that attempts to experimentally uncover the hidden rules that individuals use to make trade-offs [33–36]. Moreover, the authors in [22] suggest that studies analyzing the trade-offs in privacy behavior should employ at least one:

- Benefit variable (such as perceived benefit) which corresponds to utility in our conjoint analysis study.
- Privacy risk variable (such as information privacy concerns) corresponding to the factor "Information used by the OSN provider".
- Coping variable (such as self-efficacy and privacy control) corresponding to the factor "User privacy control".

For the purpose of this study, socio-demographic data, data related to users' self-reported habits, behavior, and concerns were collected through an online survey, alongside data collected from experimentally designed conjoint profiles related to user preferences. The analyses were made (a) to overview user behavior, concerns, and preferences solely, (b) to identify the link between socio-demographic factors and segments identified according to users' privacy intentions; and most importantly (c) to propose a new segmentation approach based on conjoint results of evaluating user preferences.

The data were collected by an online survey among 843 OSN users. The prevalent group consists of people who are currently studying or who hold a university degree. Therefore, respondents are supposed to possess an above average level of knowledge and information about the conditions and risks of using online social networks. Even though the sample expressed privacy concerns about the misuse of their data, in general, they are willing to share private data and information through online social networks. This is in line with the findings of Hugl [44].

Bearing in mind that the aim of the paper is to propose a new categorization of OSN users according to their attitudes toward privacy, we first categorized the respondents using the Westin approach in order to use it later as a reference point for the comparison with the results obtained through the proposed approach. It was found that socio-demographic factors can be some kind of predicting indicators of belonging to Westin categories. For example, the majority of women are categorized as pragmatists, whereas the majority of men are fundamentalists; younger people, single people, and those who are in a relationship are mostly pragmatists or unconcerned, while older and married people are fundamentalists. These results are in line with the results of a study related to concerns of data misuse in Europe [45]. However, the gap between predicted attitudes and self-reported behavior of respondents classified according to Westin privacy index segmentation has been noted; for instance, there are a number of fundamentalists who access applications that collect private data. In particular, only 35.3% of Westin fundamentalists never access these applications, as opposed to 42.3% of pragmatists and even 42.9% of those unconcerned.

The results of conjoint analyses showed that on average, respondents consider the popularity of an OSN and the information used by OSN providers as more important factors than privacy control options given to users and the possibility of customizing an OSN. However, two-step cluster analysis classified users into 5 clusters based on their individual preferences obtained by conjoint analysis: fundamentalists, pragmatists tending to control privacy, pragmatists, socially oriented pragmatists, and unconcerned.

Detailed analysis showed that the actual behavior of OSN users is in line with their belonging to identified CA clusters. It was also found that there is a certain correlation between the socio-demographic characteristics of the respondents and their belonging to a specific cluster. For example, women are more pragmatists and pragmatists tend to prefer privacy control, while men are more socially oriented pragmatists and unconcerned. There is an almost equal percentage of

men and women among fundamentalists. Furthermore, a high percentage of young people belong to the segment of fundamentalists, while those unconcerned included an above-average percentage of those over 45 years old and those who are married. Individuals who are in relationships mostly belong to socially oriented pragmatists. These results suggest that demography should be discussed as an important factor that, along with preferences, directly affects privacy issues. Some other researchers came to a similar conclusion, although there are contradictory findings related to certain demographic factors, especially age [5,6,8,45–48].

Cross-segment analysis has shown little match between the conjoint and Westin segments. Extreme cases are the 21 respondents who are classified as unconcerned or fundamentalists by the WPSI and who are classified into opposite clusters by conjoint segmentation. More importantly, their self-reported behaviors correspond more with the expected behavior of the conjoint clusters. For example, respondents who are classified by Westin segmentation as fundamentalists are not so protective of their privacy, which corresponds more to the CA privacy unconcerned segment. The conclusion is that that the behavior of users classified into certain clusters is in accordance with their preferences obtained as a result of conjoint analysis.

The predicted behavior of CA segment members has been shown to be consistent with their self-reported behavior. Therefore, conjoint analysis can be successfully used for the purpose of cluster indexing and even to predict the behavior of OSN users when it comes to privacy.

This paper makes a number of contributions. Let us summarize the most significant ones:

- Research based on OSN users' preferences is extended and the body of knowledge on privacy attitudes and behavior is enriched.
- Heterogeneity of OSN user preferences was identified and five cluster are isolated.
- A new more sophisticated categorization of OSN users is proposed, allowing for a more accurate prediction of privacy behavior.

However, it is important to note some limitations of the study. The first limitation involves the level of education of the respondents, which is quite high in this study. Furthermore, although the sample size is quite large and the experimental results are quite clear, the size of Cluster 5 remains debatable. Thus, a larger sample size could confirm the robustness of the proposed approach. The second limitation is the reliance on respondents' self-reported behavior when making conclusions about the privacy paradox. One of the methodological limitations of CA is related to the selection of relevant attributes and attribute levels covered by the study. Adding new factors can result in changing the number and characteristics of isolated clusters, while choosing an unbalanced number of levels can lead to their over or under estimate. Future research could focus on the collection of more data and the diversification of respondents by their country of residence, level of education, and level of awareness about risks of data misuse, as well as the collection of data on actual OSN user behavior.

Author Contributions: Conceptualization, M.K. and G.S.; methodology, M.K; validation, G.S., and M.K.; formal analysis, M.K. and G.S.; investigation, M.K. and G.S.; writing—original draft preparation, M.K. and G.S.; visualization, M.K. and G.S.; writing—review and editing, M.K. and G.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding. The APC was partially funded by the University of Belgrade, Faculty of Organizational Sciences.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. Socio-demographic data across clusters.

	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5	Sample
Gender (p = 0.024) * **						
Male	28.72%	23.53%	25.17%	34.24%	50.00%	28.59%
Female	71.28%	76.47%	74.83%	65.76%	50.00%	71.41%
Age (p = 0.007) **						
16–19	14.54%	12.25%	24.50%	11.96%	13.64%	15.18%
20–25	52.84%	58.33%	43.71%	63.59%	40.91%	54.57%
26–35	18.44%	14.22%	12.58%	11.96%	31.82%	15.30%
36–45	9.22%	12.75%	14.57%	10.33%	9.09%	11.27%
>45	4.96%	2.45%	4.64%	2.17%	4.55%	3.68%
Education (p = 0.007) **						
Primary school	2.48%	1.47%	12.58%	4.35%	4.55%	4.51%
High school	42.55%	44.12%	36.42%	40.76%	40.91%	41.40%
Undergraduate	34.75%	37.75%	32.45%	32.61%	36.36%	34.64%
Master degree	18.09%	15.20%	16.56%	19.57%	18.18%	17.44%
PhD degree	2.13%	1.47%	1.99%	2.72%	0.00%	2.02%
Occupation (p = 0.000) *						
Students (high school)	4.96%	2.94%	17.22%	4.89%	4.55%	6.64%
Students (university)	54.26%	64.22%	48.34%	65.22%	50.00%	57.89%
Unemployed	7.45%	6.86%	5.30%	4.89%	9.09%	6.41%
Employed	33.33%	25.49%	29.14%	24.46%	36.36%	28.83%
Retired	0.00%	0.49%	0.00%	0.54%	0.00%	0.24%

* $p < 0.001$; ** $p < 0.01$; *** $p < 0.05$.

Table A2. Self-reported privacy related behavior across clusters.

	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5	Sample
Sharing Intentions						
Personal Data (Real Name, Date of Birth...) * (p = 0.000) *						
All OSN users	8.51%	8.82%	6.62%	13.04%	27.27%	9.73%
Friends and their friends	5.32%	4.90%	7.28%	6.52%	31.82%	6.52%
Just friends	53.19%	59.31%	50.99%	60.33%	36.36%	55.40%
Selected friends	32.98%	26.96%	35.10%	20.11%	4.55%	28.35%
Photos (p = 0.015) **						
All OSN users	3.90%	3.43%	3.97%	3.80%	13.64%	4.03%
Friends and their friends	8.87%	6.86%	10.60%	10.87%	27.27%	9.61%
Just friends	59.93%	61.76%	58.94%	67.39%	54.55%	61.68%
Selected friends	27.30%	27.94%	26.49%	17.93%	4.55%	24.67%
Posts (p = 0.051) ***						
All OSN users	6.03%	5.88%	7.28%	4.89%	13.64%	6.17%
Friends and their friends	5.32%	6.37%	9.93%	7.61%	22.73%	7.35%
Just friends	65.96%	62.25%	57.62%	70.11%	54.55%	64.18%
Selected friends	22.70%	25.49%	25.17%	17.39%	9.09%	22.30%

Table A2. *Cont.*

	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5	Sample
Privacy Related Behaviour						
I Access Applications that Collect PersonalData *(p = 0.098)**						
Never	42.91%	40.69%	39.07%	32.07%	40.91%	39.26%
Sometimes	54.26%	55.39%	54.97%	64.13%	45.45%	56.58%
Always	2.84%	3.92%	5.96%	3.80%	13.64%	4.15%
I Access My Profile from Public Computers **(p = 0.003)						
Never	67.02%	68.63%	59.60%	55.98%	40.91%	62.99%
Sometimes	32.62%	29.41%	36.42%	41.30%	50.00%	34.88%
Always	0.35%	1.96%	3.97%	2.72%	9.09%	2.14%
I Accept Friend Requests from Strangers *(p = 0.000)						
Never	66.31%	69.61%	56.29%	60.33%	50.00%	63.58%
Sometimes	32.98%	29.41%	42.38%	37.50%	36.36%	34.88%
Always	0.71%	0.98%	1.32%	2.17%	13.64%	1.54%
Respondents' Concerns aboutPrivacy and Safety *(p = 0.000)						
Own personal data	3.24	3.1	2.98	2.9	2.05	3.05
friends' personal data	2.72	2.71	2.62	2.44	1.55	2.60

* $p < 0.001$; ** $p < 0.01$; *** $p < 0.05$.

References

1. Ali, S.; Islam, N.; Rauf, A.; Din, I.U.; Guizani, M.; Rodrigues, J.J.P.C. Privacy and security issues in online social networks. *Future Internet* **2018**, *10*, 114. [CrossRef]
2. Penni, J. The future of online social networks (OSN): A measurement analysis using social media tools and application. *Telemat. Inform.* **2017**, *34*, 498–517. [CrossRef]
3. Li, X.; Yang, Y.Y.; Chen, Y.; Niu, X. A privacy measurement framework for multiple online social networks against social identity linkage. *Appl. Sci.* **2018**, *8*, 1790. [CrossRef]
4. Hallam, C.; Zanella, G. Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Comput. Hum. Behav.* **2017**, *68*, 217–227. [CrossRef]
5. Keith, M.J.; Thompson, S.; Hale, J.; Lowry, P.B. Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *Int. J. Hum. Comput. Stud.* **2013**, *71*, 1163–1173. [CrossRef]
6. Savić, G.; Kuzmanović, M. Behaviour and Attitudes vs. Privacy Concerns of Social Online Networks. In *Knowledge Discovery in Cyberspace: Statistical Analysis and Predictive Modeling*; Kuk, K., Ranđelović, D., Eds.; Nova Publishers: Hauppauge, NY, USA, 2017; pp. 121–150.
7. Preibusch, S. Guide to measuring privacy concern: Review of survey and observational instruments. *Int. J. Hum. Comput. Stud.* **2013**, *71*, 1133–1143. [CrossRef]
8. Gerber, N.; Gerber, P.; Volkamer, M. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Comput. Secur.* **2018**, *77*, 226–261. [CrossRef]
9. Ooi, K.B.; Hew, J.J.; Lin, B. Unfolding the privacy paradox among mobile social commerce users: A multi-mediation approach. *Behav. Inform. Technol.* **2018**, *37*, 575–595. [CrossRef]
10. Li, H.; Luo, X.R.; Zhang, J.; Xu, H. Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. *Inform. Manag.* **2017**, *54*, 1012–1022. [CrossRef]
11. Choi, H.; Park, J.; Jung, Y. The role of privacy fatigue in online privacy behavior. *Comput. Hum. Behav.* **2018**, *81*, 42–51. [CrossRef]
12. Barth, S.; de Jong, M.D.T. The privacy paradox—Investigating discrepancies between expressed privacy concerns and actual online behavior—A systematic literature review. *Telemat. Inform.* **2017**, *34*, 1038–1058. [CrossRef]
13. Kumaraguru, P.; Cranor, L.F. *Privacy Indexes: A Survey of Westin's Studies*; Institute for Software Research International, School of Computer Science, Carnegie Mellon University: Pittsburgh, PA, USA, 2005.

14. Kayes, I.; Imrul, A. Privacy and security in online social networks: A survey. *Online Soc. Netw. Media* **2017**, *3*, 1–21. [CrossRef]
15. Krishnamurthy, B. Privacy and online social networks: Can colorless green ideas sleep furiously? *IEEE Secur. Priv.* **2013**, *11*, 14–20. [CrossRef]
16. Bahri, L.; Carminati, B.; Ferrari, E. Decentralized privacy preserving services for online social networks. *Online Soc. Netw. Media* **2018**, *6*, 18–25. [CrossRef]
17. Park, J.S.; Kwiat, K.A.; Kamhoua, C.A.; White, J.; Kim, S. Trusted online social network (OSN) services with optimal data management. *Comput. Secur.* **2014**, *42*, 116–136. [CrossRef]
18. Acquisti, A.; Grossklags, J. Privacy and rationality in individual decision making. *IEEE Secur. Priv.* **2005**, *3*, 26–33. [CrossRef]
19. Yao, M.Z. Self-protection of Online Privacy: A Behavioral Approach. In *Privacy Online*; Trepte, S., Reinecke, L., Eds.; Springer: Berlin/Heidelberg, Germany, 2011.
20. Joinson, A.N.; Reips, U.D.; Buchanan, T.; Paine Schofield, C.B. Privacy, trust, and self-disclosure online. *Hum. Comput. Interact.* **2010**, *25*, 1–24. [CrossRef]
21. Norberg, P.A.; Horne, D.R.; Horne, D.A. The privacy paradox: Personal information disclosure intentions versus behaviors. *J. Consum. Aff.* **2007**, *41*, 100–126. [CrossRef]
22. Li, Y. Theories in online information privacy research: A critical review and an integrated framework. *Decis. Support Syst.* **2012**, *54*, 471–481. [CrossRef]
23. Li, H.; Sarathy, R.; Xu, H. Understanding situational online information disclosure as a privacy calculus. *J. Comput. Inform. Syst.* **2010**, 62–71. [CrossRef]
24. Rogers, R.W. A protection motivation theory of fear appeals and attitude change. *J. Psychol.* **1975**, *91*, 9–114. [CrossRef] [PubMed]
25. Li, Y.; Jin, H.; Yu, X.; Xie, H.; Xu, Y.; Xu, H.; Zeng, H. Intelligent prediction of private information diffusion in social networks. *Electronics* **2020**, *9*, 719. [CrossRef]
26. Alsulami, M.M.; Al-Aama, A.Y. Employing behavioral analysis to predict user attitude towards unwanted content in online social network services: The case of Makkah region in Saudi Arabia. *Computers* **2020**, *9*, 34. [CrossRef]
27. Deuker, A. Addressing the Privacy Paradox by Expanded Privacy Awareness—The Example of Context-aware Services. In *Privacy and Identity Management for Life*; Bezzi, M., Duquenoy, P., Fischer-Hübner, S., Hansen, M., Zhang, G., Eds.; Springer: Berlin, Germany, 2010. [CrossRef]
28. Kokolakis, S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Comput. Secur.* **2017**, *64*, 122–134. [CrossRef]
29. Bergström, A. Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Comput. Hum. Behav.* **2015**, *53*, 419–426. [CrossRef]
30. Baek, Y.M. Solving the privacy paradox: A counter-argument experimental. *Comput. Hum. Behav.* **2014**, *38*, 33–42. [CrossRef]
31. Jeong, Y.; Kim, Y. Privacy concerns on social networking sites: Interplay among posting. *Comput. Hum. Behav.* **2017**, *69*, 302–310. [CrossRef]
32. Lee, N.; Kwon, O. A privacy-aware feature selection method for solving the personalization–privacy paradox in mobile wellness healthcare services. *Expert Syst. Appl.* **2015**, *42*, 2764–2771. [CrossRef]
33. Popović, M.; Vagić, M.; Kuzmanović, M.; Anđelković Labrović, J. understanding heterogeneity of students' preferences towards English medium instruction: A conjoint analysis approach. *Yug. J. Oper. Res.* **2016**, *26*, 91–102. [CrossRef]
34. Maeng, K.B.; Jung, J.; Koo, Y. Quantitative analysis of consumer preferences of windows set in South Korea: The role of energy efficiency levels. *Energies* **2019**, *12*, 1816. [CrossRef]
35. Kuzmanovic, M.; Martic, M.; Vujosevic, M. Designing a profit-maximizing product line for heterogeneous market. *Teh. Vjesn.* **2019**, *26*, 1562–1569. [CrossRef]
36. Popović, M.; Savić, G.; Kuzmanović, M.; Martić, M. Using data envelopment analysis and multi-criteria decision-making methods to evaluate teacher performance in higher education. *Symmetry* **2020**, *12*, 563. [CrossRef]
37. Valdez, A.C.; Ziefle, M. The users' perspective on the privacy-utility trade-offs in health recommender systems. *Int. J. Hum. Comput. Stud.* **2019**, *121*, 108–121. [CrossRef]

38. Krasnova, H.; Hildebrand, T.; Guenther, O. Investigating the value of privacy in online social networks: Conjoint analysis. In Proceedings of the 30th International Conference on Information Systems (ICIS 2009), Phoenix, AZ, USA, 15–18 December 2009; p. 173.
39. Kuzmanovic, M.; Savic, G.; Gusavac, B.A.; Makajic-Nikolic, D.; Panic, B. A conjoint-based approach to student evaluations of teaching performance. *Expert Syst. Appl.* **2013**, *40*, 4083–4089. [CrossRef]
40. Krane, D.; Light, L.; Gravitch, D. *Privacy On and Off the Internet: What Consumers Want*; Harris Interactive: Manchester, UK, 2002; Volume 10003, p. 15229.
41. Woodruff, A.; Pihur, V.; Consolvo, S.; Schmidt, L.; Brandimarte, L.; Acquisti, A. Would a privacy fundamentalist sell their DNA for $1000. if nothing bad happened as a result? The Westin categories, behavioral intentions, and consequences. In Proceedings of the Symposium on Usable Privacy and Security (SOUPS 2014), Menlo Park, CA, USA, 9–11 July 2014; p. 2.
42. Pu, Y.; Grossklags, J. Using conjoint analysis to investigate the value of interdependent privacy in social app adoption scenarios. In Proceedings of the International Conference on Information Systems—Exploring the Information Frontier (ICIS 2015), Fort Worth, TX, USA, 13–16 December 2015; p. 173.
43. Phelps, J.E.; D'Souza, G.; Nowak, G.J. Antecedents and consequences of consumer privacy concerns: An empirical investigation. *J. Interact. Mark.* **2001**, *15*, 2–17. [CrossRef]
44. Hugl, U. Reviewing person's value of privacy of online social networking. *Internet Res.* **2011**, *21*, 384–407. [CrossRef]
45. Cecere, G.; Le Guel, F.; Soulié, N. Perceived internet privacy concerns on social networks in Europe. *Technol. Forecast Soc. Chang.* **2015**, *96*, 277–287. [CrossRef]
46. Hoofnagle, C.J.; King, J.; Li, S.; Turow, J. *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?* (SSRN Scholarly Paper No. ID 1589864); Social Science Research Network: Rochester, NY, USA, 2010.
47. Taddicken, M. The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *J. Comput. Mediat. Commun.* **2014**, *19*, 248–273. [CrossRef]
48. Lee, H.; Wong, S.F.; Oh, J.; Chang, Y. Information privacy concerns and demographic characteristics: Data from a Korean media panel survey. *Gov. Inf. Q.* **2019**, *36*, 294–303. [CrossRef]