Chapter 15
The Cost of Using Facebook: Assigning Value to Privacy Protection on Social Network Sites Against Data Mining, Identity Theft, and Social Conflict

Wouter Martinus Petrus Steijn

15.1 Introduction

A popularity amongst millions of users worldwide has rapidly befallen social network sites (SNS) which focus on social relationships and interaction, such as Facebook. This popularity is despite the different privacy risks users are exposed to at the same time. Not only is the shared information on SNSs subject to data mining (Andrews 2012), it also exposes the user to potential identity theft as well (Noda 2009; Timmer 2009), and users have to manage different social contexts (e.g. friends, family, and colleagues) to avoid social conflict (Binder et al. 2009; Skeels and Grudin 2009). The use of SNSs is therefore often seen as evidence that users no longer care about privacy (Johnson 2010) and that users could claim their privacy important is considered paradoxical.

The paradox quickly unravels though, if one takes the social merits SNS provide for its users into account. SNS provide social merits in the forms of new possibilities for self presentation and social interactions with friends (Ellison et al. 2007; Steinfield et al. 2008). These social merits depend on where one's social network is (e.g., where one's friends are) online, leaving users with little choice what SNSs they pick. As a result, participation on SNSs is not necessarily informative of actual privacy concern.

This study will not only provide new insight in SNS users privacy concerns by describing the relative importance they attribute to different privacy threats, but will also contribute to the ongoing privacy discussion by addressing the privacy paradox and by emphasizing the need for further development of new privacy policies and regulation. An innovative method will be used to determine the relative importance attributed by SNS users to the potential privacy threats of data mining, identity theft, and social conflict. Furthermore, the degree to which younger and older individuals differ in how they attribute importance to the various threats will be investigated. To this date no research exists, to the author's knowledge, which has explicitly compared

W. M. P. Steijn (✉)
Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University,
Warandelaan 2, 5037 Tilburg, The Netherlands
e-mail: w.m.p.steijn@uvt.nl

S. Gutwirth et al. (eds.), *Reloading Data Protection*,
DOI 10.1007/978-94-007-7540-4_15, © Springer Science+Business Media Dordrecht 2014

what privacy threats users find most important. Next, some additional background will be given concerning the proposed methodology, before the research hypotheses are formulated based on related work.

15.1.1 Background

A choice based conjoint (CBC) design was chosen to investigate the relative importance SNS users attribute to different privacy threats[1]. CBC is a popular research design used in marketing to determine how a new product would best fit consumers' wishes (Curry 1996; Orme 1996). The strength of a CBC design is that it can determine the relative value respondents attribute to the features of a product avoiding direct questioning, but instead relying on respondents' actual decisions. In addition, as respondents are presented with a complete product, as opposed to for example paired wise comparison where respondents' decisions are based on only two features at the time, the decision making process can be considered more realistic

While potential privacy threats SNSs users encounter can't be included as features directly, it is easy to imagine how respondents could be presented with choice tasks between SNSs which vary on privacy protection features affecting these different potential privacy threats. This assumes that the importance users attribute to a certain privacy protection feature will be indicative of where their main privacy concerns lie. This assumption can be justified with Petronio's Communication Privacy Management (CPM) theory (2002).

CPM theory addresses the dialectical relationship between the need for privacy and the desire to share personal information with others. It describes how we create metaphorical boundaries to be able to share information with some, while excluding others to this information. These boundaries are signaled and maintained through an implicit rule-based system. For example, we whisper certain information not only to literally avoid being overheard, but also to signal to the other that what we say is private and do not wish for it to be shared with others. In effect, a boundary is formed surrounding that information including only the other to whom the information is whispered and who has become a co-owner of that information (Petronio 2002).

Although CPM focuses on the face-to-face context, the described dialectical need has become especially apparent on contemporary SNS. SNS have become an important medium and offer social merits to its users in the forms of new possibilities for self presentation and social interactions with friends (Ellison et al. 2007; Steinfield et al. 2008), resulting in large amounts of information being shared on these sites. Instead of being limited to metaphorical boundaries, SNS provide the technological tools to enforce the boundaries concerning personal information (Litt 2012). For example, by changing the settings of their posts to *friends* on Facebook, users restrict access to only their contacts and exclude anyone else who might be attempting to see what they posted on their profile. Maintaining these boundaries online has

[1] http://www.sawtoothsoftware.com/products/cbc/cbc_method

become increasingly important and necessary because the permanence and searchability of online information (boyd 2008b, p. 27) would otherwise make online shared information accessible to anyone at anytime.

The current study specifically focuses on the relative importance SNS users attribute to boundaries against the following three potential privacy threats on SNSs: data mining, identity theft, and social conflict. While users are exposed to all three privacy threats at the same time on SNSs, each threat has a different origin and other factors influence users' protection against each threat. Next, these three types of privacy threats will be briefly described in relation to SNSs and examples will be given of what privacy protection features SNSs could provide that affect that privacy threat.

Data Mining. This category concerns the potential privacy threat imposed by data mining and profiling by the SNS provider and third parties. Since the business model of SNSs is generally based on the use of the available personal information for commercial purposes, personal data placed on these sites often becomes available for companies. The scale on which data mining occurs is reflected in the economic value of Facebook as a company (Pékarek and Leenes 2009). SNSs can contain several features which affect the privacy protection of the user against data mining. First, it makes a difference whether the site owns the information posted on the site and whether information can be removed by users or remains in the database. Second, SNS generally have a policy concerning the access of third parties to personal information disclosed by the user as well.

Identity theft. This category concerns the potential privacy threats imposed by strangers with criminal intent, of which identity theft is the most familiar. Several features of SNSs can provide privacy protection against identity theft by strangers. One way is the privacy settings which only allow ones contacts to access ones full profile. However, this only provides partial protection as users are inclined to accept friend requests from strangers (Noda 2009). Another way to create boundaries against identity theft is by refraining from posting personally identifiable information online, since even posting seemingly innocent information such a the date of birth can have risks (Timmer 2009). Consequently, if SNSs require users to fill in identifying data (such as a name) or contact data (such as an email address) to verify their profile, the privacy threat of identity theft is increased.

Social conflict. This category concerns the potential privacy threat of social conflict. This is mainly a consequence of the mixed social contexts on SNSs: socializing with friends now occurs within reach of your family and (future) employers. Information shared with one group, is not necessarily appropriate or desirable to be disclosed to others and could lead to tension or conflict (Binder et al. 2009; Skeels and Grudin 2009; Lampinen et al. 2009). Several features of SNSs can affect the privacy protection of users against social conflict. First of all, being able to sort contacts into different groups and to discriminate in what information is available to what groups can help create boundaries between social context. Second, the possibility to tag pictures on SNSs can affect the boundary someone tries to protect in a negative way. An example for thiswould be a tagged picture (drunk at a party) posted by a friend becoming visible to family as well. Third, SNSs could enable users to track visitors to their profile which could expose frequent visitors. Facebook, however, does not support this option (Mongold 2010).

This study compares the relative importance attributed to privacy protection features against data mining, identity theft, or social conflict by users of SNSs of all ages. The current section has introduced the proposed methodology and grounded it in theory and operationalized the privacy threats of interest. Next, related work will be discussed in order to introduce the research hypotheses.

15.1.2 Related Work

Privacy has been a subject of research for many years, but in recent years the focus primarily lies on privacy and the internet. Not only the media (Andrews 2012; Noda 2009; Timmer 2009), but academia as well have given a lot of attention to the potential privacy threats of data mining and identity theft on SNSs. (Acquisti and Gross 2006; Debatin et al. 2009; Govani and Pashley 2005; Gross and Acquisti 2005). The studies generally concluded that their student samples of Facebook users appear not to care about the potential privacy threats on such sites. These conclusions were mainly driven by the amount of information shared by the students, despite the risks.

However, participation on SNS does not necessarily mean that users don't have any privacy concerns. The popularity of social network sites is a result of the possibilities they create for social interaction with friends (Ellison et al. 2007; Steinfield et al. 2008). Non-participation may even simply not be considered due to the related social costs in missing out on the social interactions amongst friends occurring on these sites (Raynes-Goldie 2010). As a result, even privacy concerned and aware individuals may join a SNS.

Indeed, SNSs users have proven to be creative concerning their privacy protection against social conflict (boyd and Marwick 2011, p. 14; Lampinen et al. 2009; Stutzman and Hartzog 2009), but when it comes to their boundaries against data mining and identity theft, they primarily have to rely on what the sites provide. This does not automatically suggest that they are not concerned about these potential privacy threats; there is simply little they can do if they want to socialize on these sites. The findings of Paine and colleagues (2007) support this notion. When asked, their 20-year-old and older respondents reported spam, spyware, hackers, access to personal information, and identity theft as their major privacy concerns in relation to the internet.

Respondents are therefore expected to be aware of the potential privacy threats of data mining and identity theft and attribute more importance to privacy protection features related to these aspects as opposed to features protecting against social conflict. In other words, it is expected that the fact that they are participating on SNSs does not diminish their concern about data mining and identity theft. Furthermore, respondents are expected to be unwilling to change to a different SNS provider, because they are bound to their SNS through their social network being present on that site. For this purpose the following hypotheses were formulated:

> Hypothesis 1: Respondents will generally attribute more importance to privacy protection features against data mining and identity theft than privacy protection features against social conflict.
>
> Hypothesis 2: Respondents will generally be unwilling to change to a different social network site provider.

As was discussed earlier, the fact that SNSs are most popular amongst younger individuals, does not necessarily say much since SNSs are a useful social tool for youth to accomplish several important developmental tasks: forming new friendships and creating their identity and reputation (Boneva et al. 2006; boyd 2008a; Ellison et al. 2007; Lampe et al. 2006; Madden and Smith 2010; Marwick et al. 2010). However, younger individuals are also pretty consistently found to be less concerned about their privacy compared to older individuals (Cho et al. 2009; Nowak and Phelps 1992; Paine et al. 2007).

One explanation given for this is that young and old differ in what they consider privacy to entail. Some studies reported that younger individuals might be more concerned with protecting their privacy in relation to social conflict (boyd and Marwick 2011; Livingstone 2008; Marwick et al. 2010; Raynes-Goldie 2010), as opposed to data mining and identity theft, which may become more important concerns only after individuals grow older. This would also be in line with CPM theory which states that as individuals grow older their desired privacy boundaries will evolve as well (Petronio 2002). Therefore the following hypothesis was formulated:

> Hypothesis 3: Younger respondents, compared to older individuals, will attribute more importance to privacy protection features against social conflict.

CPM theory also states that in the case of turbulence, or privacy violations, individuals will be motivated to adjust their privacy boundaries (Petronio 2002). Indeed, several studies reporting a reactive attitude of users concerning their online privacy settings. Debatin and colleagues found that respondents who actually experienced a privacy violation, as opposed to hearing about it happening from others, were more likely to take steps to protect their online privacy (2009). Similarly, Govani and Pashley concluded that raising the awareness of the privacy threats is not enough to nudge people into protecting their privacy (2007). It is therefore likely that a relationship exists between the importance individuals attribute to different privacy protection features and any negative consequences they may have experienced on SNSs. Thus, the following hypothesis was formulated:

> Hypothesis 4: Respondents who have experienced a negative consequence from using SNS will attribute more importance to privacy protection related to that experience.

15.2 Method

This study employed choice-based conjoint (CBC) analysis in order to be able to compare the relative importance attributed to various privacy protection features. In a traditional CBC design, respondents are given several discrete choice tasks of

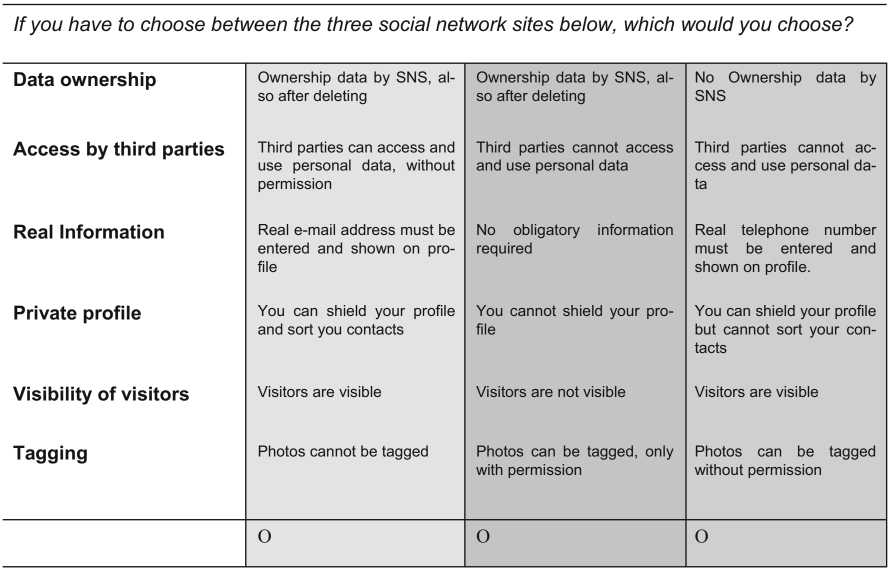
Table 15.1 Overview of all features and levels used in the choice-based conjoint study

Feature	Level	
Data ownership	No ownership of data by SNS	O1
	Ownership of data by SNS, until deleting profile	O2
	Ownership of data by SNS, also after deleting profile	O3
Access by third parties	Third parties cannot access and use personal data	A1
	Third parties can only access and use personal data with permission	A2
	Third parties can access and use personal data without permission	A3
Real information	No obligatory information necessary	I1
	Real email-address must be entered, but not obligatory shown on profile	I2
	Real email address must be entered, and must be shown on profile	I3
	Real telephone number must be entered, but not obligatory shown on profile	I4
	Real telephone number must be entered, and must be shown on profile	I5
Private profile	Private profile and sorting of contacts	S1
	Private profile but no sorting of contacts	S2
	No private profile and no sorting of contacts	S3
Visibility of visitors	Profile visitors are not visible	V1
	Profile visitors are visible	V1
Tagging	Photos cannot be tagged.	T1
	Photos can be tagged, only with permission	T2
	Photos can be tagged, without permission	T3

selecting a concrete offering out of a selection of products with several features which differ over several levels. This could for example concern pizza's, which vary in the features price (e.g., with the levels cheap versus expensive), size (e.g., large versus small), toppings (e.g., cheese versus salami) and brand (e.g. unknown versus familiar). The respondents would be presented with several different pizza's and asked which they would be most likely to buy. When the resulting trade-off decision is repeated several times, the relative value of each feature can be determined; will people buy a pizza based on the price or the brand?In addition, it ccan be determined which level of these features is most preferred; do they rather have cheese or salami as a topping.

For the current study, respondents were presented with several scenarios depicting hypothetical SNSs and were asked on which SNS they would prefer to create a profile. The SNSs varied based on 6 features affecting online privacy: *data ownership, access by third parties, real information, private profile, visibility of visitors,* and *tagging*. An overview of the features and the levels in which the features will vary during the discrete choice tasks are shown in Table 15.1.

Generally, all features included a level for the presence or absence of a privacy protective setting or policy. An additional level was added for *data ownership*, *access third parties*, *private profile*, and *tagging* in which the user had control over the



If you have to choose between the three social network sites below, which would you choose?

Data ownership	Ownership data by SNS, also after deleting	Ownership data by SNS, also after deleting	No Ownership data by SNS
Access by third parties	Third parties can access and use personal data, without permission	Third parties cannot access and use personal data	Third parties cannot access and use personal data
Real Information	Real e-mail address must be entered and shown on profile	No obligatory information required	Real telephone number must be entered and shown on profile.
Private profile	You can shield your profile and sort you contacts	You cannot shield your profile	You can shield your profile but cannot sort your contacts
Visibility of visitors	Visitors are visible	Visitors are not visible	Visitors are visible
Tagging	Photos cannot be tagged	Photos can be tagged, only with permission	Photos can be tagged without permission
	O	O	O

Fig. 15.1 This is an example of the screen respondents were presented

feature. The feature *real information* included levels which varied in the sensitivity of the information required to be provided (i.e. an email-address versus a telephone number) and whether the obligatory information should also be visible on the profile.

Each of these features affects the privacy protection against data mining, identity theft, or social conflict differently. The features *data ownership* and *access by third parties* primarily concern the protection against data mining. The features *tagging* and *visibility of visitors* concern the protection against social conflict. The feature *private profile*, however, affects both identity theft—is the profile private or not- and social conflict—can the user sort his contacts in different groups or not. Similarly, the feature *real information* affects both data mining—is contact information obligatory or not- and identity theft—should contact information be shown on the profile or not.

The SNSs were presented to respondents in the form of an online survey. The online survey was conducted by the research institute TNS-NIPO[2] by means of the CAWI-method (computer assisted web interviewing), which allows respondents to participate from their own computer at home. The survey consisted of three parts.

The first part contained instructions that explained the content of the survey. All features and their levels were explained in the instruction, to get all respondents to have a similar understanding of what the different levels entail.

The second part consisted of the actual discrete choice tasks. Respondents were presented with 15 discrete choice tasks each. Each task consisted of three different SNSs from which respondents had to pick the one they preferred. Figure 15.1 shows

[2] www.tns-nipo.com

Table 15.2 Age gender, and profile of respondents across age groups

	12–13	14–15	16–19	20–25	26–30	31–40	41–50	50 +	Total
N	66	68	66	77	67	67	71	78	560
Age	12.6	14.5	17.2	22.5	28.2	35.5	44.9	62.5	30.4
Gender (male)	42.4 %	42.6 %	40.9 %	40.3 %	31.3 %	44.8 %	39.4 %	50.0 %	41.6 %
Facebook	6.1 %	16.2 %	24.2 %	42.9 %	41.8 %	31.3 %	29.6 %	34.6 %	28.8 %
Hyves	48.5 %	13.2 %	9.1 %	6.5 %	3.0 %	4.5 %	11.3 %	19.2 %	14.3 %
Both	45.5 %	70.6 %	66.7 %	50.6 %	55.2 %	64.2 %	59.2 %	46.2 %	57.0 %

an example of a discrete choice task as presented to the respondents. All possible combination of levels were equally represented throughout the experiment.

The third part contained a short questionnaire with several follow-up questions to further explore the motivation behind the choices participants made. First, respondents were asked to indicate which of the features had been most important for them in making their decisions. Next, respondents were asked if they were willing to switch to another social network site provider. If so, they were subsequently asked what their primary reason would be. Lastly, two yes/no questions asked respondents whether they were specifically concerned about something when using their profile and whether they have had a negative experience due to using their profile. When answered with a yes, respondents were further prompted to describe what exactly they were concerned with or have experienced. Subsequent responses were categorized as *Misuse information, Privacy* (e.g. greater visibility or other general statements about privacy), *Criminals* (e.g. hackers or burglars), *undesired contact, social conflict* (e.g. bullying or fights), or *other* (e.g. technical problems). Four raters categorized the responses independently and inter-rater reliability were acceptable for both *concerns* (Kappa's ranging from .727 to .807) and *negative experiences* (Kappa's ranging from .626 to .694). Disagreements were resolved through discussion.

15.2.1 Participants

Respondents were recruited from participants of an earlier study concerning privacy and user behavior on social network sites and obtained by means of a stratified sampling procedure. Five hundred and sixty respondents (327 female, 233 male, $M_{age} = 30.36$, $SD = 16.83$) completed the survey. Table 15.2 provides an overview of age and gender distribution over all age groups. All respondents are members of Facebook or Hyves. Respondents were rewarded for their participation with credits through which they can obtain coupons at TNS-NIPO. Informed consent was obtained from all respondents and parents provided consent for respondents younger than 18-years-old.

15.2.2 Analysis Plan

TNS-NIPO makes use of the simulation tool 'Valuemanager' for conjoint analysis, which provides two statistics of interest: (1) *importance percentages*, (2) *utility scores* (see also Orme 2010, chap. 9). An importance percentage is calculated for all six features. This percentage is an estimation of how many decisions were primarily based on that feature. The importance percentages of all features will add up to 100. The utility score provides the relative importance for each level within a feature. This utility score can't be compared between features, but within a certain feature one can determine which level was preferred most (provided the most utility) by respondents in their decisions. The utility scores of the levels within a feature add up to 0. As a result, a negative utility does not necessarily mean that that a specific level was disliked; other levels within that feature were simply preferred.

In order to analyze the importance percentages obtained through conjoint analysis and other percentages, one sample t-tests between percents were used. For the comparison between groups one-way ANOVA's and χ^2 analysis were used. Bonferroni post hoc analysis were used to examine significant one-way ANOVA results, whereas the adjusted standardized residuals were compared for significant χ^2's. Some analysis only involved a sub group of the total sample and therefore violated the assumption of χ^2 analysis that each cell should hold a minimum of 5 individuals. To avoid this, dummy variables were made of separate answer categories and only three age groups were used: 12–19-year-olds, 20–30-year-olds, and 31 and older.

15.3 Results

15.3.1 Importance Percentages and Utilities

Before testing the first hypothesis, the utility scores were inspected to gain some insight in the decision patterns of respondents. Table 15.3 shows that rather than each feature having a level that was clearly preferred over the others, each feature has a level that is clearly less preferred compared to the other levels. This means that their decisions were primarily based on avoiding certain levels, as opposed to picking SNSs which contained at least a certain level of privacy protection.

Only for *tagging* a clear preference for a certain level seems to exist as well; tagging should be possible, but only with permission (T2). Concerning the other features, the respondents clearly disfavored SNS where: SNS had ownership over the data, also after deleting the profile (O3), third parties can access and use personal data without permission (A3), a real telephone number must be provided, and must be shown on profile (I5), access to the profile cannot be limited to contacts only, and where the contacts cannot be sorted into groups (S3), profile visitors are visible (V1), and photos can be tagged without permission (T3).

The utilities show that the levels that provide control to the respondent (in the form of having to give permission) were most preferred. Furthermore, the utilities concerning the feature *real information*, suggest that respondents were primarily

Table 15.3 Utility scores obtained through conjoint analysis

Features	Level	Utility
Data Ownership	O1	34,5
	O2	24,0
	O3	−58,5
Access by third parties	A1	26,0
	A2	36,4
	A3	−62,3
Real information	I1	36,1
	I2	46,5
	I3	−22,7
	I4	21,5
	I5	−81,4
Private profile	S1	32,2
	S2	21,9
	S3	−54,0
Visibility of Visitors	V1	0,5
	V2	−0,5
Tagging	T1	0,4
	T2	19,7
	T3	−20,1

See Table 15.2 for the content of the levels

concerned with having to show contact information on their profile rather than having to share a telephone number with the SNS per se. Requiring a telephone number to create a profile was preferred over the requirement of a visible email address, but a required (not visible on the profile) email address was preferred over no required information at all. This suggests that respondents had little problem with providing contact information to the SNSs.

Next, the importance percentages obtained through conjoint analysis were investigated to test the first hypothesis that respondents would attribute more importance to privacy protection from data mining and identity theft. *Real information* was deemed most important (26.4 %). Followed by *data ownership* (20.8 %), *access by third parties* (19.6 %), *private profile* (16.6 %), *tagging* (11.6 %), and *visibility of visitors* (5.0 %). These percentages support the hypothesis that respondents attribute most importance to privacy protection data mining and identity theft. The features concerning privacy protection against data mining and identity theft, i.e. *real information, data ownership,* and *access by third parties*, determined the decision of respondents in 66.8 % of all discrete choice tasks which is significantly more often than the remaining features which primarily concerned social conflict, $t(559) = 8.44$, $p < .001$.

The responses to the question which of the features had been most important for respondents in making their decisions, shows a rather different picture from the one presented by the importance percentages obtained through the conjoint analysis. Only 10 % of respondents reported *real information* to be the most important feature for their decisions whereas 44.3 % of all respondents reported *private profile* to be the most important feature.

Table 15.4 Importance percentages obtained through conjoint analysis and self reported importance attributed to features for decision making

	Importance percentage	Self reported importance (%)
Real information	26.4 %	10.0 %
Data ownership	20.8 %	26.4 %
Access by third parties	19.6 %	11.1 %
Private profile	16.6 %	44.3 %
Tagging	11.6 %	1.6 %
Visibility of visistors	5.0 %	3.6 %
None/Don't know	–	1.3 %

Table 15.4 provides both the importance percentages obtained through conjoint analysis and the percentage of individuals reporting what feature was most important for their decisions. When comparing the self reported importance of the features for decision making with the through conjoint analysis obtained importance percentages of the features, a clear discrepancy can be seen. While respondents claim that the feature *private profile* was most important for their decisions, the importance percentages suggest that three other features have actually been more important instead in their actual decisions.

15.3.2 Willingness to Switch SNS

Next, the second hypothesis was explored: that respondents would generally be unwilling to change to a different SNS provider. In total 201 (35.9 %) respondents indicated they would be willing to switch. Responses to the question when they would be willing to switch could be grouped in several categories. Most respondents willing to switch mentioned they would change only if their friends would change as well (36 %) or if their privacy was better protected at the other site (33 %). Alternatively, respondents would be willing to switch if the other site might be easier, better, or more fun (20.3 %), or they would switch for another reason (10.7 %). Of the 359 (64.1 %) respondents not willing to change, the most often heard reason was that they were satisfied with their current SNS (54.2 %), followed by, that it would cost too much time and effort (10.2 %), they are using their current profile little as it is (9.6 %), it would result in even more information on the internet (3.1 %), and other reasons (8.2 %).

These results provide support for the second hypothesis as the majority of respondents indicated to be unwilling to switch to a different SNS provider. Furthermore, a third of the respondents willing to change will only do so if their current social network (i.e. their friends) switches as well.

15.3.3 Age Based Differences for Importance Percentages

The third hypothesis stated that in comparison to older individuals, younger individuals would attribute more importance to privacy protection against social conflict. Investigation of the importance percentages did not provide support for this hypothesis. Although one-way ANOVA showed a significant age effect for *tagging*, F (7,552) = 2.307, *p* = .025, post hoc analysis did not indicate a significant difference between any of the age groups. Furthermore, no age effect was found for *real information*, F (7,552) = 1.817, *p* = .082, *data ownership*, F (7,552) = 1.271, *p* = .262, *access by third parties*, F (7,552) = .583, *p* = .770, *private profile*, F (7,552) = 1.275, *p* = .260, and *visibility of visitors*, F (7,552) = .778, *p* = .606.

Similarly, investigation of the self-reported importance of the features with χ^2 analyses showed little to no support for the hypothesis. A significant age effect was found for *access by third parties*, χ^2 (7, 560) = 16.60, *p* = .020, and for *visibility of visitors*, χ^2 (7, 560) = 21.51, *p* = .003. Significantly more 41–50-year-olds and respondents older than 50 reported these features to be most important for their decisions. No age effect was found for *data ownership*, χ^2 (7, 560) = 11.14, *p* = .133, *real information*, χ^2 (7, 560) = 5.99, *p* = .540, *private profile*, χ^2 (7, 560) = 11.57, *p* = .115, and *tagging*, χ^2 (7, 560) = 6.44, *p* = .489.

To summarize, no concrete differences were found between the age groups concerning the importance percentages obtained through analysis and the self reported importance of the features. Which means that not only all respondents of all ages similalry reported which feature was most important for their decision making, but they also made similar decisions during the discrete choice tasks resulting in similar importance percentages. Subsequently, the discrepancy between the importance percentages obtained through analysis and the self reported importance of the features is similar as well for respondents of all ages.

15.3.4 Concerns and Experienced Negative Consequences

First, respondents' responses to what they were concerned about when using SNSs were investigated. Of all respondents, 228 (40.7 %) reported to be concerned with something when using their profile. Table 15.5 provides an overview of what respondents were concerned with. Overall, significantly fewer 12–19-year-olds (32 %) reported to be concerned when using their profile compared to 20–30-year-olds (52.8 %) and respondents 31-years-old and older (41.2 %), χ^2 (4, 560) = 18.64, *p* = .001.

Privacy was mentioned as a concern most often (41.2 %) followed by *misuse information* (32.5 %), *criminals* (12.3 %), *undesired contact* (7.0 %), *social conflict* (4.8 %) and *other* (2.2 %). Significantly more respondents 31 and older and fewer 12–19-year-olds were concerned about *misuse information*, χ^2 (2, 228) = 9.72, *p* = .008. No age differences were found in the number of respondents who were concerned with *privacy,* χ^2 (2, 228) = 4.94, *p* = .085, *criminals,* χ^2 (2, 228) = 4.29, *p* = .117.

Table 15.5 Reported concerns or experienced negative consequences from using social network sites

	12–19	20–30	30 +	Total
Concerns				
N	64	76	88	228
Misuse information	21,9 %	27,6 %	44,3 %	32,5 %
Privacy	34,4 %	51,3 %	37,5 %	41,2 %
Criminals	10,9 %	18,4 %	8,0 %	12,3 %
Undesired contact	17,2 %	1,3 %	4,5 %	7,0 %
Social Conflict	12,5 %	1,3 %	2,3 %	4,8 %
Other	3,1 %	0,0 %	3,4 %	2,2 %
Experienced				
N	35	15	31	81
Misuse information	0,0 %	13,3 %	16,1 %	8,6 %
Privacy	17,1 %	6,7 %	22,6 %	17,3 %
Criminals	2,9 %	20,0 %	3,2 %	6,2 %
Undesired contact	5,7 %	26,7 %	19,4 %	14,8 %
Social Conflict	57,1 %	20,0 %	22,6 %	37,0 %
Other	17,1 %	13,3 %	16,1 %	16,0 %

Due to the low number of respondents *undesired contact, social conflict,*and *other* could not be reliably analyzed, although a trend is visible in Table 15.5 that 12–19-year-olds more often reported the former two.

Eighty-one respondents (14.5 %) reported to have actually experienced a negative consequence from their presence in a SNS. Table 15.5 shows what negative consequences were experienced by respondents. No age differences were found in number of respondents reporting negative experiences, χ^2 (2, 560) = 3.39, $p = .183$.

Social conflict was the most reported negative experience (41.2 %), followed by *privacy* (17.3 %), *other* (16.0 %), *undesired contact* (14.8 %), *misuse information* (8.6 %) and *criminals* (6.2 %). The low number of respondents does not allow for a reliable comparison between the age groups. However, a higher percentage of 12–19-year-olds reported *social conflict*, while fewer 12–19-year-olds reported *undesirable contact* and *misuse information. Privacy* and *criminals* were reported by more 20–30-year-olds.

These results suggest that differences do exist between the online experience of privacy of younger and older individuals in line with the expectations of hypothesis 3. Respondents 12–19-year-old appear to be more concerned about social conflict, and report to have experienced it more often.

Finally, to investigate hypothesis 4 which predicted a relationship between the attribution of importance to privacy protection features and experienced negative consequences, the relationship between negative experiences and the importance percentages obtained from analysis was explored. A significant relationship was found between the reported negative experiences and the feature *data ownership*. Respondents who reported to have experienced a negative experience had a significantly higher importance percentage (23.6 %) for the feature *data ownership* than respondents who reported not to have experienced a negative experience (20.3 %), F (1,559) = 6.330, $p = 0.012$.

Further investigation showed that only respondents who experienced misuse of their information attributed more importance to *data ownership*. The importance percentage for these respondents was 35.1 % as opposed to the average importance percentage of 23.6 %. However, due to the low number of respondents involved in this analysis, the results did not achieve statistical significance. Therefore, only marginal support was found for the hypothesis. No statistical significant relationship was found between reported concerns and attributed importance to the various privacy protection features.

15.4 Discussion

This article's main objective was to compare the relative importance SNS users attribute to privacy protection against data mining, identity theft, and social conflict. The presented results show that respondents of all ages attribute most importance to privacy protection against data mining and identity theft. Furthermore, respondents display decision patterns primarily aimed at avoiding obvious privacy violations as opposed to achieving the best possible privacy protection. The implications of these results will be further discussed next.

As was stated in the first hypothesis, respondents were found to attribute most importance to privacy protection features against data mining and identity theft. Thus, SNS users' privacy concerns appear to match the privacy threats given most attention by academia and media alike (Acquisti and Gross 2006; Andrews 2012; Debatin et al. 2009; Govani and Pashley 2005; Gross and Acquisti 2005; Noda 2009; Timmer 2009). This suggests that all respondents were at least to some degree aware of the possible dangers and thus the importance of protection against these potential privacy threats.

In the introduction, it was argued that individuals' online behavior should not be used as gradient for their privacy concerns, because SNSs are primarily used for the possibilities they create for social interaction (Ellison et al. 2007; Steinfield et al. 2008). Indeed, only a third of respondents reported to be willing to switch in line with the second hypothesis. Furthermore, a third of those willing to switch reported explicitly that they would only switch if their social network (of friends) would switch as well, further supporting that participation is generally based on the social merits these sites provide and the choice of SNSs thus largely depends on where the social network of the individual is present.

In other words, the social utility of SNSs appears to be the primary reason individuals make use of the sites and thus have to accept the potential privacy threats as a cost for participation. Given the massive popularity of SNSs- Facebook has over 1 billion users[3]- non-participating may even be associated with social costs by individuals as they miss out on the social interaction (Raynes-Goldie 2010). As a result even privacy concerned individuals are likely to participate on SNSs. Since the business model of SNSs depends on their users sharing information as openly

[3] Statistic from newsroom.fb.com

as possible (Andrews 2012; Pékarek and Leenes 2009), safeguarding the privacy of their users can not be considered their priority.

No support was found for the third hypothesis which stated that younger respondents would attribute more importance to protection features against social conflict. Neither the importance percentages obtained through conjoint analysis, nor the self reported importance attribution differed significantly between younger and older respondents. The hypothesis was based on CPM theory predicting differences between desired privacy boundaries as age progresses (Petronio 2002) and previous studies suggesting youth to be more concerned about their privacy in relation to social conflict with known others (boyd and Marwick 2011; Livingstone 2008; Marwick et al. 2010; Raynes-Goldie 2010). Only the fact that more 12–19-year-olds reported fears or negative consequences related to social conflict provides some support that these privacy concerns play a bigger role for youth.

A possible explanation for the lack of differences between the age groups concerning the importance attributed to the privacy protection features could be that users have numerous other tools to safeguard their privacy concerning social conflict. Even without the features used in this study, youth can safeguard their privacy concerning social conflict by using multiple sites, or by using more private channels for more intimate interactions (boyd and Marwick 2011, p. 14; Lampinen et al. 2009; Stutzman and Hartzog 2009). Conversely, users are fully dependent on the settings and policies provided by the SNS platform concerning their privacy protection against data mining and identity theft, especially if deception is not possible or desirable. As a result, even if younger individuals are more concerned to avoid social conflict they may still have prioritized their privacy protection against data mining and identity theft in this study, because they have no control over these forms of privacy other than the features the SNS provides.[4]

The lack of differences between age groups does suggest that even young respondents are aware of the importance of privacy protection features on SNSs against data mining and identity theft. It is noteworthy that respondents of all ages (i.e. even 12-year-olds and adults) attributed similar importance to all privacy protection features. Especially since younger individuals are often considered to care less about their privacy than adults. These results suggest that SNS users of all ages still attribute importance to their privacy protection from data mining and identity theft, even though their use of SNSs makes them vulnerable to these threats.

A distinctive pattern was found in the utility scores. Instead of demonstrating a clear preference, respondents instead demonstrated a clear dislike (relative to the other levels) for a certain level of each feature. In other words, respondents' decisions during the discrete choice tasks were not necessarily based on obtaining a certain ideal SNS concerning privacy protection, but mainly on avoiding unacceptable privacy violations. When looking at *real information*, for example, respondents didn't primarily pick the SNSs in which they didn't have to fill in any information (in fact having to provide an email address, not shown on the profile was most preferred),

[4] New developments like the Google dashboard may give users more control in time in this respect. Google Dashboard promises users more transparency and control concerning the information linked to their google accounts. https://accounts.google.com

but mainly avoided those SNSs which required them to show the information on their profile. At that point the privacy situation apparently became unacceptable for respondents.

The previously described decision pattern seems related to the fact that individuals often take active steps to protect their privacy after an incident. A negative incident is often the first clear sign that the privacy protection was lacking. Therefore, individuals may be under the impression that their privacy protection is good enough until it is too late. Either because they lack of accurate knowledge on how well protected they are (Hoofnagle et al. 2010) or don't expect to be singled out amongst all the other SNS users (e.g. "Safety in numbers", see Grimmelman 2009, p. 1161). As a result, individuals can be expected to only take action once their lacking privacy protection has become visible through a negative experience, as opposed to continuously trying to obtain the best privacy protection.

Here, however, only marginal support was found for the fourth hypothesis that respondents importance attribution to privacy protection features would related to experienced negative consequences. Respondents who reported their data having been misused, did attribute more importance to the feature *data ownership,* but not statistical significance was obtained. This could be the result of the low number of respondents reporting to have experienced a negative consequence, or could simply mean that this relationship does not exist. Future studies may want to explore this more elaborately.

The focus on avoiding unacceptable privacy violations might also be related to the discrepancy found between what conjoint analysis produced as main features for decision making, i.e. *real information*, *data ownership*, and *access third parties,* and what respondents reported to be the main feature, i.e. *private profile*. Although the former three features were the most prominent for decision making according to conjoint analysis, the decision for these features may have been made by rules of thumb: if the level to be avoided was present, that SNS would not be chosen. As mentioned before, for the feature *private profile,* numerous alternatives exist for SNS users to protect their privacy, while for the other three features concerning data mining and identity theft they are primarily dependent on what the SNS provides.

In this study, respondents apparently first and foremost tried to avoid the undesired levels for *real information*, *data ownership*, and *access third parties*. This decision may have been made relatively easy in the respondents' mind. The subsequent decision if two or more SNSs would still be left, would have to be based on the remaining features. This aspect of decision making may have been more prominent for respondents and as a result indicate the feature *private profile* as most important for decision making.

15.4.1 Limitations

This study made use of a CBC design to assess the privacy attitudes of SNS users. The used levels in this experiment are rather long compared to usual discrete choice tasks making the decision making more difficult. When discrete choice models become too complex, respondents could resort to simplified decision strategies. Instead of assessing the entire scenario, they will mainly focus on one or two features that are important to them. In this case it could have occurred for *real information,* and especially for the level which required a telephone number to be provided which would be visible on the profile. This may have been particularly unacceptable, causing some respondents to base their decision primarily on this.

A second limitation is the fact that the presented SNSs consisted of only privacy related features. No features were included concerning the services a SNS provides (e.g., gaming or interaction possibilities), possible costs (e.g., monthly fee), or other concerns (e.g., safety). The aim of the current study was to distinguish the attributed importance to privacy protection from various risks. Additional non-privacy related features would have made the SNSs too big for respondents to make repeated concentrated rational decisions. Therefore, no conclusions can be drawn on how important privacy protection is in relation to the provided services, costs, or other concerns. Future studies might want to do a similar set up with non-privacy related features in order to investigate the relative importance of privacy protection in relation to these other factors.

15.5 Conclusion

The results showed that respondents of all ages attribute more importance to privacy protection features against data mining and identity theft than social conflict. Here it was argued, that SNSs are used for their social merits and individuals generally have little choice on what SNSs to use. As a results, users are dependent on the SNS platform to provide the necessary privacy protection against the various privacy threats of data mining and identity theft. Lack of these features does not necessarily mean that the users no longer care about these privacy threats, as the results here demonstrated.

A recent initiative, The Brussels Privacy Declaration[5], calls attention to the need for regulation of privacy rights online. The results presented here further support the urgency for the development of regulation of online privacy. Even though SNS users are aware of the importance of privacy protection against data mining and identity theft, they generally do not optimize their privacy protection. Instead, they appear to settle for what they perceive as good enough, which is avoiding the obvious and worst privacy violations. In addition, users are generally dependent on the service provider concerning what privacy protection is available. As such the need for regulation is great; SNS users cannot be expected to protect their own privacy optimally, certainly if the only way to perfectly maintain the online boundaries is by not participating.

[5] Brusselsdecleration.net

15.6 Funding

The research reported in this chapter was partially funded by the Netherlands Organization for Scientific Research (NWO).

References

Acquisti, A., and R. Gross. 2006. Imagined communities: Awareness, information sharing, and privacy on the facebook. Paper presented at the 6th Workshop on Privacy Enhancing Technologies, Cambridge, UK.

Andrews, L. 2012. Facebook is using you. The New York Times. http://www.nytimes.com. Accessed 5 Jul. 2012.

Binder, J., A. Howes, and A. Sutcliffe. 2009. The problem of conflicting social spheres: Effects of network structure on experienced tension in social network sites. Paper presented at the CHI, Boston, M.A.

Boneva, B.S., A. Quinn, R.E. Kraut, S. Kiesler, and I. Shklovski. 2006. Teenage communication in the instant messaging era. In *Computers, phones, and the internet: Domesticating information technology,* eds. R. Kraut, M. Brynin, and S. Kiesler 201–218. Oxford: Oxford University Press.

boyd, d.m. 2008a. Facebook's privacy trainwreck: Exposure, invasion and social convergence. *Convergence* 14 (1): 13–20.

boyd, d.m. 2008b. Taken out of context: American teen sociality in networked publics. Doctoral Diss., Berkeley, University of California. http://www.danah.org/papers/TakenOutOfContext.pdf.

boyd, d.m., and A. E. Marwick. 2011. Social privacy in networked publics: Teens' attitudes, practices, and strategies. A decade in internettime: Symposium on the dynamics of the internet and society. http://ssrn.com/abstract=1925128.

Cho, H., M. Rivera-Sánchez, and S.S. Lim. 2009. A multinational study on online privacy: Global concerns and local responses. *New Media Society* 11 (3): 395–416.

Curry, J. 1996. Understanding conjoint analysis in 15 minutes. *Sawtooth Software Research Paper Series.* Sequim, WA: Sawtooth Software.

Debatin, B., J. P. Lovejoy, A. Horn, and B. N. Hughes. 2009. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer Media Communication* 15 (1): 83–108.

Ellison, N. B., C. Steinfield, and C. Lampe. 2007. The benefits of facebook "friends": Social capital and college students' use of online social network sites. *Journal of Computer Media Communication* 12 (4): 1143–1168.

Govani, T., and H. Pashley. 2005. Student awareness of the privacy implications when using facebook. http://citeseerx.ist.psu.edu/viewdoc/download?doi=2010.2001.2001.2095.6108&rep=rep2001&type=pdf. Accessed Sep. 2007.

Grimmelmann, J. 2009. Saving Facebook. *Iowa Law Review* 94:1137–1206.

Gross, R., and A. Acquisti. 2005. Information revelation and privacy in online social networks. Paper presented at the proceedings of the ACM Workshop on Privacy in the Electronic Society, Alexandria, Virginia, USA.

Johnson, B. 2010. Privacy no longer a social norm, says Facebook founder. *The Guardian.* http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy. Accessed 14 Nov. 2011.

Hoofnagle, C., J. King, S. Li, and J. Turow. 2010. How different are young adults from older adults when it comes to information privacy attitudes & policies? http://ssrn.com/abstract=1589864.

Lampe, C., N.B. Ellison, and C. Steinfield. 2006. A Face(book) in the crowd: social searching vs. social browsing. *Proceedings of CSCW-2006,* 161–170. New York: ACM Press.

Lampinen, A., S. Tamminen, and A. Oulasvirta. 2009. "All my people right here, right now": Management of group co-presence on a social networking site. Paper presented at the International Conference on Supporting Group Work (GROUP'09), Sanibel Island, Florida, USA.

Litt, E. 2012. Privy to privacy on social network sites: Another digital divide. Paper presented at the Amsterdam Privacy Conference, 2012, Amsterdam, The Netherlands.

Livingstone, S. 2008. Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society* 10 (3): 393–411.

Madden, M., and A. Smith. 2010. *Reputation management and social media*. Pew Internet and American Life Project report. http://pewinternet.org/~/media//Files/Reports/2010/PIP_Reputation_Management.pdf.

Marwick, A. E., D. M. Diaz, and J. Palfrey. 2010. Youth, privacy and reputation. Berkman Center Research Publication No. 2010–2015; Harvard Public Law Working Paper No. 2010–2029. http://ssrn.com/abstract=1588163.

Mongold, B. 2010. Facebook Privacy—Can you track who visits your profile? *Five Free Apps*. http://www.fivefreeapps.com/2010/01/facebook-privacy-can-you-track-who-visits-your-profile.html. Accessed 16 Jul. 2012.

Noda, T. S. 2009. Facebook still a hotbed of identity theft, study claims. PCWorld. http://www.pcworld.com. Accessed 5 Jul. 2012.

Nowak, G. J., and J. E. Phelps. 1992. Understanding privacy concerns: an assessment of consumers' information-related knowledge and beliefs. *Journal of Direct Marketing* 6 (4): 28–39.

Orme, B. 1996. Which conjoint method should I use? Sawtooth Software Research Paper Series. Sequim, WA: Sawtooth Software.

Orme, B. 2010. Getting started with conjoint analysis: Strategies for product design and pricing research. Madison: Research Publishers LLC.

Paine, C., U-D. Reips, S. Stieger, A. Joinson, and T. Buchanan. 2007. Internet users' perception of 'privacy concerns' and 'privacy actions'. *Human-Computer Studies* 65:526–536.

Pekárek, M., and R. Leenes. 2009. *Privacy and social network sites: Follow the money*. Paper presented at the W3C workshop on the future of social networking, Barcelona, Spain.

Petronio, S. 2002. *Boundaries of privacy: Dialectics of disclosure*. Albany: State University of New York Press.

Raynes-Goldie, K. 2010. Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday* 15 (1).

Skeels, M. M., and J. Grudin. 2009. When social networks cross boundaries: A case study of workplace use of Facebook and LinkedIn. Paper presented at the International Conference on Supporting Group Work (GROUP'09), Sanibel Island, Florida, USA.

Steinfield, C., N. B. Ellison, and C. Lampe. 2008. Social capital, self-esteem, and use of online social network sites: A longitudinal analysis. *Journal of Applied Developmental Psychology* 29 (6): 434–445.

Stutzman, F. D., and W. Hartzog. 2009. Boundary regulation in social media. http://ssrn.com/abstract=1566904.

Timmer, J. 2009. New algorithm guesses SSNs using date and place of birth. Arstechnica. http://arstechnica.com. Accessed 5 Jul. 2012.