Configuration Behavior of Restrictive Default Privacy Settings on Social Network Sites

Analyzing the Combined Effect of Default Settings and Interface Style

Markus Tschersich(✉)

Deutsche Telekom Chair of Mobile Business and Multilateral Security,
Goethe University Frankfurt, Theodor-W.-Adorno-Platz 4,
60323 Frankfurt am Main, Germany
markus.tschersich@m-chair.de

Abstract. Research about privacy in the context of social network sites has not addressed yet how users behave with restrictive default privacy settings. Literature about default settings and the sharing of personal information in social network sites lacks empirical insight into how restrictive default privacy settings influences the behavior of users. To gain empirical insight, a social network site privacy interface prototype was built to investigate the influence of default settings and interface style on the privacy configuration behavior of users. Results show configuration behavior differences between participants having restrictive or permissive privacy default settings. Further, interfaces with multiple pages of privacy settings induce participants to keep their default settings.

Keywords: Social Network Site · Privacy by Default · Privacy · Default setting · Interface

1 Introduction

Research in the area of privacy is a growing field in the information systems literature [1]. Current research about privacy in the context of social network sites (SNS) has not addressed yet how restrictive default privacy settings that do not share personal information without the explicit decision of the users, influences the behavior of users. Research strands about user behavior with software defaults and the sharing behavior of users are contradictory in the case of restrictive default privacy setting.

Literature in the field of default settings emphasizes that owing to several reasons like e.g. lack of awareness [1] and laziness [2,3], users tend to keep default settings. Consequently, when users of SNS behave similarly, more restrictive default privacy settings could lead to less shared personal information on SNS. On the other hand, users register to SNS in order to share personal information with others. This satisfies their needs to lower feelings of loneliness and to

J. Garcia-Alfaro et al. (Eds.): DPM/SETOP/QASA 2014, LNCS 8872, pp. 77–94, 2015.
DOI: 10.1007/978-3-319-17016-9_6

increase feelings of social capital [4]. On SNS with restrictive default privacy settings users cannot satisfy these needs without actively deviating from the default.

Users perform a privacy calculus by weighing between the benefits and costs of revealing personal information [5], before actually revealing personal information. Throughout this decision process and driven by their need to share personal information, users often underestimate possible risks owing to an “it wont happen to me” mentality [6]. By contrast, concepts like Privacy by Default (PbDef) [7] aim to prevent users from potential privacy threats. PbDef obliges platform providers to have the most restrictive privacy option as the preselected one for all settings that manage the revelation of personal information [8]. In online services that process personal information (like SNS), the most restrictive option is that no-one could access personal information besides the owner of the information itself. To grant other users access to personal information, everybody needs to decide explicitly what and with whom she/he wants to share.

Privacy professionals promote PbDef as a powerful concept to reduce the risk of privacy violation of the users that are also caused by the underestimation of risks by users [8,9]. Therefore, privacy professionals suggest the implementation of PbDef to all services that work with personal information. The European Commission shares the opinion of privacy professionals about the potentials of PbDef to protect the rights of citizens. Thus, as part of the European Union legislation process the European Commission and the European Parliament passed the draft law that makes PbDef binding for online service providers [10].

Providers of SNS expect PbDef to have a negative impact on the functionality of the platform and their business models [11]. The success of SNS, however, is determined by user participation, especially by sharing personal information [12]. Thus, concerns of providers are grounded in expecting less user participation owing to PbDef with its restrictive default privacy settings.

Findings of both research strands (status quo, users need) are contradictory in the case of restrictive default privacy settings and literature lacks empirical insight into how users really behave on SNS with restrictive default privacy settings and how different privacy settings influence the configuration behavior of their privacy. To provide first insights regarding this topic, our research analyzes how users differ in their configuration behavior of privacy settings by having different restrictive default privacy settings. To identify impacts by the interface we analyze the combined effect with different interface styles. This also enables a better assessment of concerns and chances of PbDef regulation in the case of SNS. To do so, we first describe the theoretical background of our research and our hypotheses in Sect. 2. Following that, in Sect. 3 we presente our methodology, including a description of our research prototype to execute the study. Section 4 presents the data collected during the study and the results of the tests. In Sect. 5 the results, implications and limitations are discussed followed by a conclusion in Sect. 6.

2 Theoretical Background

Various aspects in the field of privacy on SNS are covered in the literature [12–14]. SNS are defined to be about profiles and the connection between users [15]. Studies investigated how self-disclosure on SNS is influenced by gender [16] or culture [17] as well as what kind of personal information users disclose on their profiles on SNS [17]. Further, research investigates and describes the decision-making process performed by users before revealing personal information on SNS. The privacy calculus describes that users are performing a trade-off between the benefits and costs of their self-disclosure on SNS prior to the decision of whether to disclose personal information or not [1,6,18,19]. It is also found that trust plays an important role in this decision-making process, because it influences the perceived benefits and costs of the revelation [13].

Research also investigated why users share personal information within communities [5,20,21] and how they handle their privacy settings [22–24]. Users participate on SNS owing to several reasons. They desire identification within the community and have a need for self-verifying feedback from the community [25]. Therefore, it is important for them to present themselves within the community [26,27]. Further, communicating and sharing personal information on the SNS brings users plenty of social capital [28] and reduces feelings of loneliness [5,29].

Default settings have been investigated in numerous different domains and fields of application. Influences have been identified in the configuration of security settings of WiFi access points [30], in the purchase of seat reservations on railways [31], to the percentage of organ donors [32] and to response rates in web surveys [33]. The common theme is that users tend to accept default settings, so that defaults can also be seen as a de facto regulation [30]. Literature about opt-in and opt-out also confirms that users tend to keep preselected options [3]. Literature puts this behavior down to the status quo bias [4,34].

Several possible reasons for not changing the default settings and keeping the status quo exist: cognitive and physical laziness; perceiving default settings as correct; perceiving endorsement from the provider; or using defaults as a justification for choice [3,4,35–37]. In the case of privacy settings in SNS, literature shows that permissive default privacy options keep users off from configuring their privacy settings [23]. Having a plethora of reasons for not changing default settings, we expect that users with restrictive or permissive default settings will tend to keep close to their preselected default privacy settings. Therefore, we hypothesize:

H1: Users with restrictive or permissive default privacy settings differ in their configuration behavior of privacy settings on SNS.

When privacy settings are spread over multiple pages, users can have difficulties in getting an overview of their own privacy configurations. Further, a broader understanding of their own sharing behavior is limited [38,39]. Thus, overall complexity can be increased by more privacy settings and a finer granulation [39]. An increased complexity will reduce the transparency of the interface that will also lead users to keep their default settings [2]. Higher complexity of an interface can also require more technical skills to understand the interface [2]. Thus, the style of an interface can also affect the configuration behavior by users of their privacy settings. Therefore, we hypothesize:

H2: Users having a structured or unstructured interface differ in their configuration behavior of privacy settings on SNS.

The previously described findings about user behavior in the context of default settings and different interface styles also indicate a combined effect. Therefore, we hypothesize:

H3: Users having different restrictive default privacy settings and using a different interface differ in their configuration behavior of privacy settings on SNS.

3 Methodology

Hypotheses were checked in an experimental setting with an independent-measures study design. As our independent variables, we have two dimensions each with two conditions. The first dimension concerns the restrictiveness of the default settings. Each participant is assigned to either Privacy by Default with the preselected option that only the user herself can see her own personal information; or the opposite, that the whole SNS can see the personal information of the user. The second dimension concerns the interface. Each participant is assigned either to have all privacy settings in a list on one page or categorized in a menu with multiple pages. Based on the two dimensions with their conditions, four different groups have been built in the intersections of the conditions as displayed in Fig. 1.

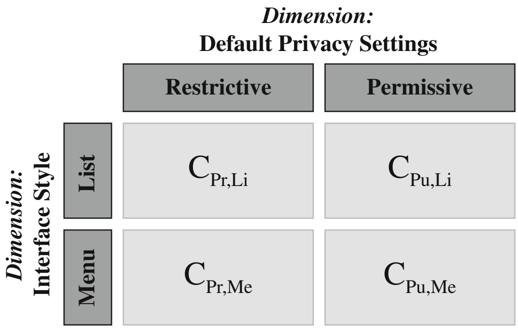


Fig. 1. Experimental groups

We analyzed the differences among the four groups for 14 different privacy settings of SNS. Relevant privacy settings were collected and clustered based on SNS that are popular in Germany: Facebook, Google+, LinkedIn, Xing, and StudiVZ. From the pool of privacy settings of these SNS, we selected for our analysis those settings that allow drawing conclusions regarding the personality of a user (e.g. personality, location, etc.). The selected settings were clustered with regard to their functionality. This results in three categories: Profile Information, Status Updates, and Media. The selected privacy settings and their grouping according to the identified categories are shown in Table 1.

Table 1. Analyzed privacy settings

Cat.	No.	Privacy settings
Profile information	1	Who can see the date of your birthday?
	2	Who can see your year of birth?
	3	Who can see whether you are interested in boys or girls?
	4	Who can see your relationship status?
Status updates	5	Who is allowed to see your status updates?
	6	Who will be informed about changes in your profile?
	7	Who is allowed to see updates about your location?
	8	Who is allowed to add information to your timeline?
	9	Who is allowed to see entries on your timeline added by others?
	10	Who is allowed to tag you in status updates?
	11	Who is allowed to tag you in photos?
Media	12	Who is allowed to see your photo albums?
	13	Who is allowed to see the location of your photos?
	14	Who is allowed to see your videos?

The dependent variable of the configuration behavior of participants is measured by the selected privacy option for each setting. Every participant can choose between options with different access rights for their personal information.

3.1 Participants

We focused on students with an active account on a social network. Overall 632 students participated in the study. An a priori power analysis with an expected effect size of r = .50 computed a required total sample size of at least 420 (105 per group) participants to get a power of .95 [40]. We met the requirements of the power analysis with our sample size of a total of 632 participants, as shown in Table 2.

Participants were motivated to participate in the study by prizes raffled among all participants that worked with the privacy interface prototype and filled out a subsequent questionnaire. Table 2 shows the distribution of the participants into the four experimental groups as well as their gender, age, and the period of time they have been using SNS. The proportion of male and female participants is comparable among all four groups. Likewise, the average ages as well as the time of SNS usage are similar within all four experimental groups.

Table 2. Sociodemographic data

	$\mathbf{C}_{Pr,Me}$	$\mathbf{C}_{Pr,Li}$	$\mathbf{C}_{Pu,Me}$	$\mathbf{C}_{Pu,Li}$	Total
Participants	115	198	126	193	632
Male	64	115	70	114	363
Female	46	73	53	77	249
No anser	5	10	3	2	20
Age					
Average Age	20.09	21.21	21.57	20.82	20.96
SD	5.33	5.97	6.65	4.61	5.63
SNS usage					
Average Years	4.78	4.91	4.81	4.70	4.81
SD	2.33	2.32	2.46	2.18	2.34

The frequency of using SNS for private purposes is comparable for all experimental groups as displayed in Fig. 2. About 70 % of the participants allocated to the interface style with privacy settings in the form of a list visit SNS several times a day. In the groups having a menu interface style the proportion of participants visiting SNS every day is over 60 %. The other participants, for the most part, visit SNS at least several times a week. Consequently, participants of our study have a high experience with SNS owing to the high frequency of their usage.

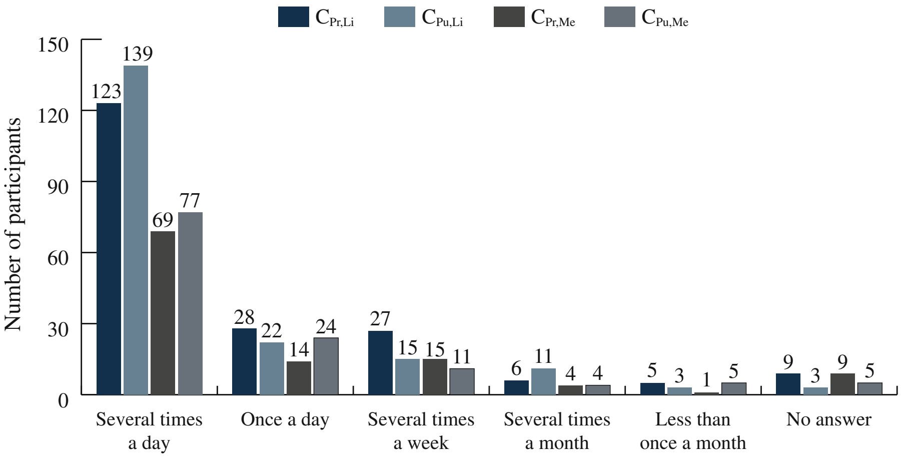


Fig. 2. Frequency of SNS usage

In addition, the distribution of the number of friends is also similar for all experimental groups, as shown in Fig. 3. Only a small portion of participants

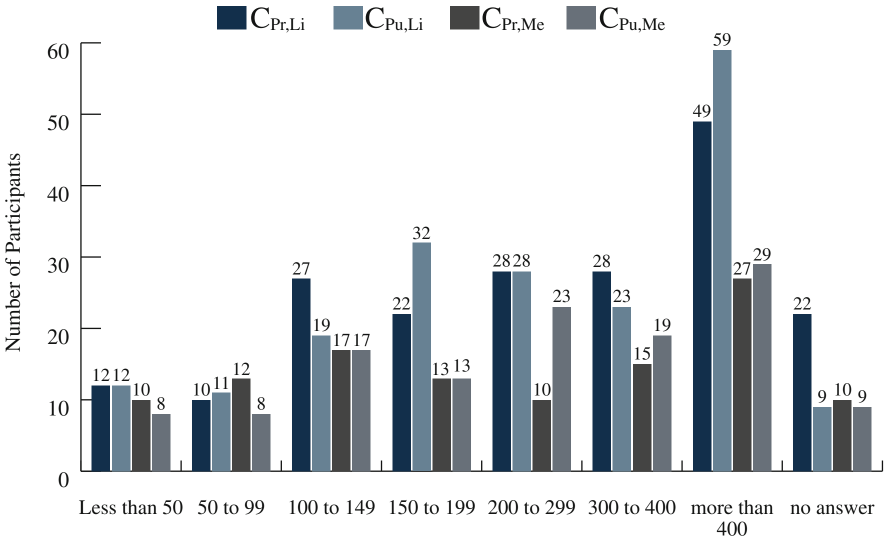


Fig. 3. Number of friends on SNS

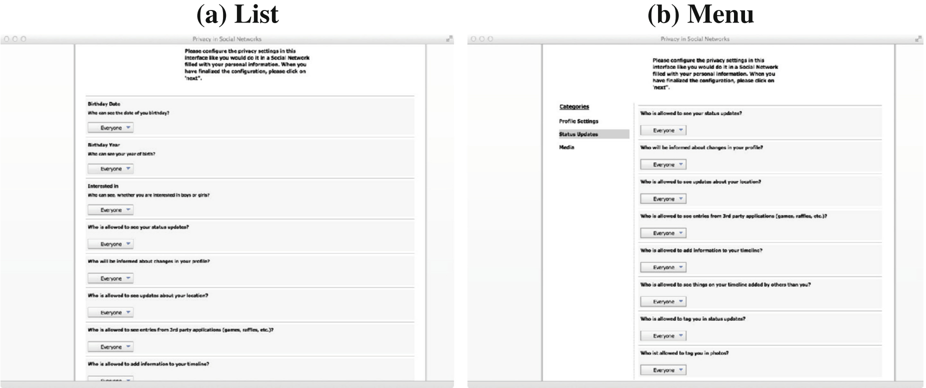
per group have fewer than 100 friends on SNS. About 30 % of all experimental groups have more than 400 friends. The rest of the participants have from 100 to 400 friends.

3.2 Privacy Interface Prototype

A Privacy Interface Prototype was built to collect the needed data for the analysis. The developed prototype is built based on web-technologies that are platform-independent. After the development, the prototype was tested with all popular web browsers.

The prototype gives the opportunity to simulate the privacy configuration interfaces from SNS based on the two analyzed dimensions, but also to display instructions and questionnaires before and after the privacy interface. Furthermore, the prototype measures the duration that participants spend on each page. Participants can move between the pages through buttons at the bottom of each page.

The privacy configuration interface is composed of those privacy settings that are part of our analysis. To test the influence of the interface style, two different layouts of interfaces, as shown in Fig. 4 can be displayed by the prototype. In the first layout that simulates the interface style of (a) List, all analyzed privacy settings are laid out one below the other. In the second layout that simulates the interface style of (b) Menu, the analyzed privacy settings are spread over multiple pages grouped by the identified categories. The category Profile Information is displayed as the first page after starting the privacy interface prototype. With a menu on the left side participants can navigate between the pages of the categories to configure those privacy settings.



(a) List

Privacy in Social Networks

Please configure the privacy settings in this interface like you would do it in a Social Network filled with your personal information. When you have finalized the configuration, please click on "next".

Birthday Date
Who can see the date of you birthday?
Everyone ▾

Birthday Year
Who can see your year of birth?
Everyone ▾

Interested in
Who can see, whether you are interested in boys or girls?
Everyone ▾

Who is allowed to see your status updates?
Everyone ▾

Who will be informed about changes in your profile?
Everyone ▾

Who is allowed to see updates about your location?
Everyone ▾

Who is allowed to see entries from 3rd party applications (games, raffles, etc.)?
Everyone ▾

Who is allowed to add information to your timeline?

(b) Menu

Privacy in Social Networks

Please configure the privacy settings in this interface like you would do it in a Social Network filled with your personal information. When you have finalized the configuration, please click on "next".

Categories
Profile Settings
Status Updates
Media

Who is allowed to see your status updates?
Everyone ▾

Who will be informed about changes in your profile?
Everyone ▾

Who is allowed to see updates about your location?
Everyone ▾

Who is allowed to see entries from 3rd party applications (games, raffles, etc.)?
Everyone ▾

Who is allowed to add information to your timeline?
Everyone ▾

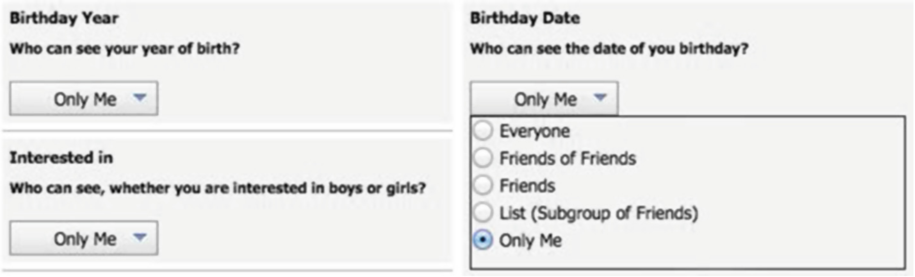
Who is allowed to see things on your timeline added by others than you?
Everyone ▾

Who is allowed to tag you in status updates?
Everyone ▾

Who ist allowed to tag you in photos?
Everyone ▾

Fig. 4. Screenshots of the privacy interface prototype

Independently of the interface style, next to the description of each privacy setting a button exists to configure the privacy setting. A pull-down menu opens by clicking on this button and shows all available options as demonstrated in the example of restrictive default privacy settings in Fig. 5. In this menu each participant has the opportunity to choose between the following privacy options: (1) Everybody, (2) Friends of Friends, (3) Friends, (4) List (Subgroup of Friends), or (5) Only me. Initially, the default value based on the particular condition is shown on the button. Participants can change the privacy settings until they finalize the whole session of the privacy interface prototype and move to the next page with a questionnaire. When an option is changed, the button shows the latest selected option and this option is saved to the database of the prototype.



Birthday Year
Who can see your year of birth?
Only Me ▾

Interested in
Who can see, whether you are interested in boys or girls?
Only Me ▾

Birthday Date
Who can see the date of you birthday?
Only Me ▾
○ Everyone
○ Friends of Friends
○ Friends
○ List (Subgroup of Friends)
● Only Me

Fig. 5. Configuration of privacy settings

3.3 Procedure

Participants were asked to open the website with the privacy interface prototype in their web-browser. Initially, a page with instructions was shown describing the procedure of the study and instructing participants that the privacy interface requires them to configure privacy settings as they would do it on SNS with their personal information. Regarding the purpose of the study, participants were informed that we want to understand how they configure their privacy settings on SNS. They were not told that we are especially focusing on their configuration behavior with regard to different default privacy settings and interface styles.

On the next page, the interface of the privacy settings was displayed to the participants. In this step, the participants were randomly allocated to one of the four experimental groups based on both analyzed dimensions with each of the two conditions. For those experimental groups ($\mathrm{C}_{Pr,Li}$, $\mathrm{C}_{Pr,Me}$) that have the condition of restrictive default settings the option Only me was preselected to all privacy settings as proposed by PbDef. For the other experimental groups ($\mathrm{C}_{Pu,Li}$, $\mathrm{C}_{Pu,Me}$) we simulated the opposite - that all personal information is available on the SNS. The privacy settings of participants had been set to the option Everybody as the preselected option. Besides the default setting and based on the second analyzed dimension, participants had been allocated to one of the previously described interface styles.

All experimental groups were now asked to configure their privacy settings accordingly to their preferences, but were not forced to change any of the settings. Participants could quit the session of the privacy settings configuration by clicking on the button *Next* to move forward to the next page. Following that, they were asked some questions regarding their age, gender and usage behavior on SNS. Figure 6 summarizes the procedure of the study.

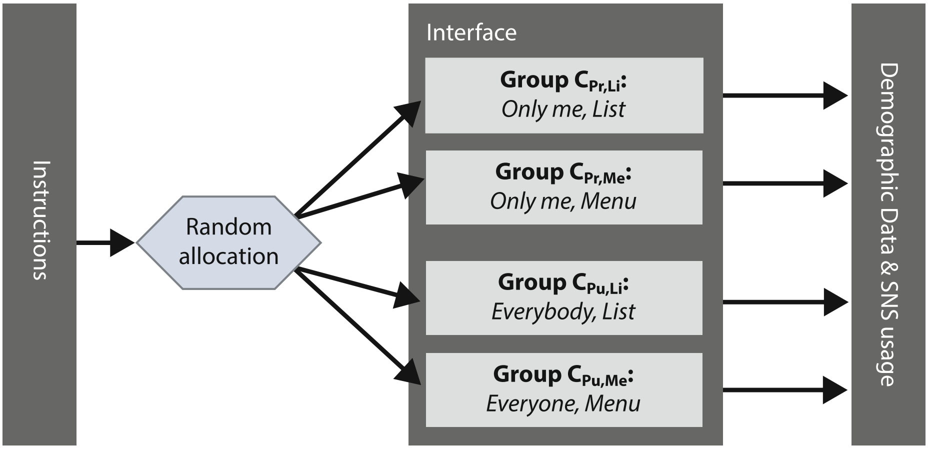

Instructions
Random allocation
Interface
Group C_Pr,Li: Only me, List
Group C_Pr,Me: Only me, Menu
Group C_Pu,Li: Everybody, List
Group C_Pu,Me: Everyone, Menu
Demographic Data & SNS usage

Fig. 6. Procedure of the study

4 Results

For each of the 14 analyzed privacy settings the participants had been able to choose from the previously described five options. It was required to code the

Table 3. Coding of privacy options

Code	Value
1	Everybody
2	Friends of Friends (FoF)
3	Friends
4	List (Subgroup of Friends)
5	Only me

privacy options to be able to run statistical analysis. We coded the options from 1 (Everybody) to 5 (Only me) as shown in Table 3.

In the following, descriptive statistics as well as the results of the statistical test are described in more detail.

4.1 Descriptive Statistics

For each of the analyzed privacy settings, we calculated the mean and the standard deviation based on the collected and coded data. This was done for all four experimental groups separately. Results for all groups are listed in Table 4. A separate comparison for each interface style shows that groups with restrictive default privacy settings ($C_{Pr,Li}$, $C_{Pr,Me}$) have a higher mean than groups with permissive settings ($C_{Pu,Li}$, $C_{Pu,Me}$). The difference between the means is even higher for the menu interface layout compared to the list layout. Standard deviations for each setting are comparable for all groups.

4.2 Comparison of Privacy Configuration Behavior

To test our hypothesis, an adequate statistical test is required to identify differences in our experimental groups based on two predictor variables: Default Privacy Setting and Interface Layout. Parametric tests that compare the ratio of systematic variance (e. g. Two-Way Independent ANOVA) require homoscedasticity [41]. Based on the results of Leven's test we found that this assumption was not fulfilled. Therefore, we used the Scheirer-Ray-Hare (SHR) test [42], a non-parametric alternative that allows to analyze the combined effect of two predictor variables. This ranking-based test is more conservative compared to the parametric Two-Way Independent ANOVA, but it allows investigation of the combined effect, even for the presence of heteroscedasticity. The SHR test gives results about the significance of the effect on the privacy configuration behavior of each analyzed dimension separately and of the combined effect. A p-value of $p < .05$ implies that H0 can be rejected under the 5-percent level. According to this a p-value of $p > .05$ implies that we have to reject the tested hypothesis.

As displayed in Table 5, results show the significant effect of the default setting on the configuration behavior for all 14 analyzed privacy settings. Therefore, we can see hypothesis H_1 as fulfilled. Further, results show that a significant effect

Table 4. Descriptive statistics

No.	$\mathbf{C}_{Pr,Li}$		$\mathbf{C}_{Pu,Li}$		$\mathbf{C}_{Pu,Me}$		$\mathbf{C}_{Pr,Me}$	
	$\bar{x}$	SD	$\bar{x}$	SD	$\bar{x}$	SD	$\bar{x}$	SD
1	3.05	1.06	2.73	1.11	2.61	1.19	3.17	1.06
2	3.53	1.29	2.93	1.34	2.94	1.44	3.49	1.31
3	3.58	1.44	2.67	1.47	2.87	1.57	3.32	1.58
4	3.48	1.23	2.89	1.31	2.82	1.19	3.30	1.16
5	2.99	0.74	2.73	0.78	1.65	0.98	4.11	1.00
6	3.70	1.04	3.20	1.09	1.90	1.39	4.50	0.88
7	3.93	1.06	3.40	1.26	1.98	1.51	4.61	0.78
8	3.52	0.97	2.87	0.98	1.67	1.01	4.15	1.00
9	3.49	1.08	2.80	1.02	1.63	0.98	4.17	1.03
10	3.35	0.95	2.89	0.89	1.73	1.09	4.26	0.97
11	3.47	0.98	2.92	0.98	1.77	1.15	4.30	0.92
12	3.19	0.82	2.86	0.83	1.69	1.00	4.23	0.97
13	3.78	1.07	3.17	1.15	1.72	1.11	4.44	0.92
14	3.55	1.07	3.03	0.99	1.74	1.10	4.26	1.06

Table 5. Results of Scheirer-Ray-Hare test

No.	Default setting		Interface style		Default*Interface	
	df	p-value	df	p-value	df	p-value
1	1	.000	1	.886	1	.596
2	1	.000	1	.880	1	.590
3	1	.000	1	.710	1	.092
4	1	.000	1	.128	1	.392
5	1	.000	1	.003	1	.000
6	1	.000	1	.648	1	.000
7	1	.000	1	.157	1	.000
8	1	.000	1	.661	1	.000
9	1	.000	1	.263	1	.000
10	1	.000	1	.119	1	.000
11	1	.000	1	.227	1	.000
12	1	.000	1	.034	1	.000
13	1	.000	1	.073	1	.000
14	1	.000	1	.412	1	.000

on the configuration behavior is measured only for privacy settings concerning the access to timeline updates and access to photo albums. We need to reject hypothesis H_2 for the 12 privacy settings with a p-value of $p > .05$.

For all analyzed privacy settings allocated to categories Status Updates and Media a significant combined effect of the Default Setting and the Interface style is measured. There is no significant combined effect on privacy settings in the category *Profile Information.* Thus, we need to reject hypothesis H_3 for the four privacy settings of category Profile Information, but results confirm the hypothesis H_3 for privacy settings in categories Status Updates and Media.

5 Discussion

The aim of this study was to understand how users' configuration behavior of default privacy settings is affected by the restrictiveness of default settings and the style of privacy interfaces. Results show a significantly different privacy configuration behavior between the participants of the groups having restrictive ($C_{Pr,Li}$, $C_{Pr,Me}$) or permissive ($C_{Pu,Li}$, $C_{Pu,Me}$) default privacy settings. Independent of interface styles, users tend to keep close to the preselected options or to keep default settings. This applies to all 14 analyzed privacy settings of our study. Thus, results are in line with research about users' behavior with default settings in other domains [2–4].

However, the dimension of the interface style does not have a significant effect on the configuration behavior of the participants for all settings. Besides the privacy settings for the access to status updates and photo albums, a significant difference between interface style list ($C_{Pr,Li}$, $C_{Pu,Li}$) and menu ($C_{Pr,Me}$, $C_{Pu,Me}$) is measured for none of the analyzed privacy settings. This is the result of similar behavior for the two experimental groups in each interface style that can clearly be seen in the radar chart (Fig. 7). The two experimental groups having the interface style of list (solid lines) are both close to the option Friend. Experimental groups having the interface style of menu (dotted lines) are in general both oriented to the preselected options of *Everybody* and *Only me.*

Results for the combined effect of both analyzed dimensions show a significant change in the configuration behavior of privacy settings in the categories *Status Updates* and *Media.* For these settings, the difference between experimental groups having restrictive or permissive default privacy settings is also influenced by the conditions of the interface style. As displayed in Fig. 7, at least for the categories *Status Updates* and *Media*, the difference between mean values having the interface style of list is smaller than the difference between mean values having the interface style with multiple pages. For the privacy settings of the category *Profile Information* the mean values of all four experimental groups are close to each other. That results in the non-significant result of the combined effect.

Based on the test results of the combined effect, it can be concluded that users having an interface with multiple pages tend to keep default settings for the analyzed privacy settings of the categories *Status Updates* and *Media.* Analysis of the

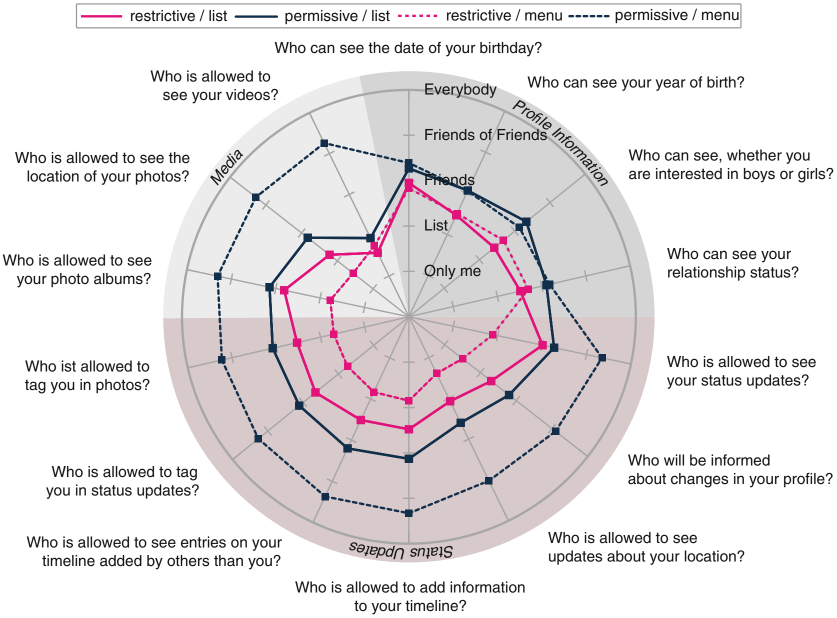


Fig. 7. Mean values of experimental groups per privacy setting

settings of category *Profile Information*, shows that participants are more willing to deviate from the default. We presume that this effect is less due to the settings themselves, but more due to the order of the categories. The category of *Profile Information* was the first page shown to the participants after starting the privacy interface prototype. Thus, participants were able to configure theses privacy settings directly. To adjust the privacy settings of the other categories they had to switch actively to another page, what was most probably not done by the majority of participants. This is in line with related research that less transparency is one reason for users to keep default settings [2]. Furthermore, higher granularity and placing settings on multiple pages can increase the complexity of the interface [39]. If users do not have enough technical skills to compensate for the higher complexity, it will also result in keeping their the default settings [2].

One can summarize, that also in the case of restrictive default privacy settings the status quo bias cannot be overcome by users' needs that require a deviation from the defaults. An interface style with multiple pages strengthens this effect on those pages that are not shown directly to the users.

5.1 Implications for Regulators and Platform Providers

Results of our study show that users behave differently whether they have restrictive or permissive default privacy settings. Concerns of platform providers seems to be confirmed that users will share less personal information in the case of PbDef. Users will share their personal information to a smaller number of addressees due to the more restrictive privacy settings. This will reduce the overall exchange of personal information within the network that could be critical for the success of the SNS [43].

Hence, the privacy settings configuration behavior of users also depends on the interface style. In the more transparent interface (list) the majority of participants favored the option that their friends can access their personal information for the majority of analyzed privacy settings. The main motivator for users to use SNS is the exchange of personal information with their friends [27]. In the case of transparent privacy settings users are still able to fulfill their need for social capital, enjoyment, and relationship-maintenance even in the case of restrictive default privacy settings [13,29]. Therefore, the concerns of SNS providers regarding the functionality of the platform are for the most parts unfounded.

Hence, problems can occur by having PbDef in the case of a less transparent privacy interface. By having permissive default privacy setting a less transparent privacy interface can increase the amount of shared personal information compared to less shared default settings [2] even it is not in line with the expectations of users. In the case of PbDef SNS providers need to increase the transparency of the privacy interface to support users in fulfilling their needs in SNS. That also implies a deviation from restrictive default privacy settings.

Expectations of the EC on PbDef can be seen as fulfilled based on the results of the study. Users that are not deviating from their default setting e.g. owing to less transparent interfaces are still protected from an unintended revelation until they are able to adjust privacy settings according to their needs and requirements. Hence, business innovation or business models are also not blocked by PbDef regulation.

5.2 Limitations

The study is limited to several aspects. The analyzed sample is limited to students. Even though literature shows that younger persons use SNS more often than older ones [44] other generations are also of interest. Literature describes a relationship between age and the number of friends on SNS [45] and that younger users have more friends compared to older ones. Both findings depict a difference in usage behavior between generations. Therefore, the results of this study might not be applicable to other age groups of SNS users. Additionally, cultural aspects could also have a relevant effect on the configuration behavior of privacy settings. Especially, settings like sexual-orientation or relationship-status could be more sensitive in other cultures compared to the Western-Europe (German) culture [13].

Our study focused on SNS used in a private context. SNS with a private focus (e.g. Facebook) differ in their requirements and characteristics from business SNS (e.g. LinkedIn) or corporate SNS [46,47]. Furthermore, personal information like sexual-orientation or relationship status are also not relevant in a professional context. Therefore, the configuration behavior of privacy settings can deviate.

The analyzed effect of the privacy configuration behavior of users is based on short-term decisions. In a real life scenario, users might be motivated to deviate from restrictive default settings at a later point in time, owing to the comments of their peers, the media or other external pressures. Thus, we cannot necessarily conclude the long-term behavior of users. Further, the behavior of the participants could be biased by the fact that due to the design of the study their personal information is never threatened. In a scenario where personal information are affected by their decision behavior is might be different.

Additionally, the prototype of our study was just composed out of the privacy interface. Usually, privacy interfaces of current SNS are hidden in the options or menus, besides other options. Therefore, aspects like awareness of privacy settings in general are not be covered by the results.

5.3 Future Research

As mentioned before, it is needed to identify the long-term effect of default privacy settings on the privacy configuration behavior of users on SNS. In addition, the effect of default privacy settings in interfaces with multiple pages needs further investigations. The order of analyzed categories in the interface needs to be randomized to find out whether the effect of keeping default settings is grounded in the order of categories or in the privacy settings themselves.

To counteract less shared personal information owing to restrictive default privacy settings in privacy interfaces with multiple pages, research is needed to build better interfaces. Requirements need to be identified and design guidelines need to be built to improve transparency in those privacy interfaces. Furthermore, open research fields include how experiences with SNS, the frequency of usage or the privacy sensitivity of users correlates with the configuration of privacy settings by having more restrictive default privacy settings.

6 Conclusion

With our study of 632 participants in an experimental setting, we gained empirical insight into the field of restrictive default privacy settings in the context of SNS. We built a better understanding of differences in privacy configuration behavior based on default settings or the interface style.

The findings of our study show that users' configuration behavior by users of privacy settings on SNS differs depending on the preselected option of privacy settings. Furthermore, the style of the privacy interface also partly influences the configuration behavior of privacy settings by users. Privacy interfaces with multiple pages keep users from changing their default settings, whereas interfaces that have all privacy settings in a list are more transparent and support users in deviating from the default option to adjust the privacy settings according to their needs.

Concluding, our study also demonstrate that in the case of restrictive default privacy settings users' needs that require the revelation of personal information also do not outweight the status quo bias. Having an interface style with less transparency strengthens this effect on those privacy settings that need further clicks to be accessible.

References

1. Smith, H.J., Dinev, T., Xu, H.: Information privacy research: an interdisciplinary review. MIS Q. **35**(4), 989–1016 (2011)
2. Shah, R.C., Kesan, J.P.: Policy through software defaults. In: Proceedings of the 2006 International Conference on Digital Government Research, pp. 265–272. Digital Government Society of North America (2006)
3. Bellman, S., Johnson, E.J., Lohse, G.L.: On site: to opt-in or opt-out?: it depends on the question. Commun. ACM **44**(2), 25–27 (2001)
4. Samuelson, W., Zeckhauser, R.: Status quo bias in decision making. J. Risk Uncertain. **1**(1), 7–59 (1988)
5. Burke, M., Marlow, C., Lento, T.: Social network activity and social well-being. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1909–1912. ACM (2010)
6. Dinev, T., Hart, P.: An extended privacy calculus model for e-commerce transactions. Inf. Syst. Res. **17**(1), 61–80 (2006)
7. Cavoukian, A.: Privacy by design (leading edge). IEEE Technol. Soc. Mag. **31**(4), 18–19 (2012)
8. Cavoukian, A.: Privacy by design (2008). http://privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf
9. Schaar, P.: Privacy by Default: Airbag für die Informationsgesellschaft (2009). https://www.bfdi.bund.de/bfdi_forum/showthread.php?t=3365
10. European Parliament. Report on the proposel for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (2014). http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA7-2013-0402%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN#title1
11. Europe versus Facebook. Facebook's views on the proposed data protection regulation (2012). http://www.europe-v-facebook.org/FOI_Facebook_Lobbying.pdf
12. Brooks, L., Anene, V.: Information disclosure and generational differences in social network sites (2012)
13. Krasnova, H., Veltri, N.F.: Privacy calculus on social networking sites: explorative evidence from germany and USA. In: 2010 43rd Hawaii International Conference on System Sciences (HICSS), pp. 1–10. IEEE (2010)
14. Litt, E.: Understanding social network site users privacy tool use. Comput. Hum. Behav. **29**(4), 1649–1656 (2013)
15. Boyd, D.M., Ellison, N.B.: Social network sites: definition, history, and scholarship. J. Comput. Mediated Commun. **13**(1), 210–230 (2008)
16. Taraszow, T., Aristodemou, E., Shitta, G., Laouris, Y., Arsoy, A.: Disclosure of personal and contact information by young people in social networking sites: an analysis using facebook profiles as an example. Int. J. Media Cult. Polit. **6**(1), 81–101 (2010)
17. Nosko, A., Wood, E., Molema, S.: All about me: disclosure in online social networking profiles: the case of facebook. Comput. Hum. Behav. **26**(3), 406–418 (2010)

18. Chellappa, R.K., Sin, R.G.: Personalization versus privacy: an empirical examination of the online consumers dilemma. Inf. Technol. Manage. **6**(2–3), 181–202 (2005)
19. Culnan, M.J., Bies, R.J.: Consumer privacy: balancing economic and justice considerations. J. Soc. Issues **59**(2), 323–342 (2003)
20. Ellison, N., Steinfield, C., Lampe, C.: Spatially bounded online social networks and social capital. Int. Commun. Assoc. **36**, 1–37 (2006)
21. Lampe, C., Ellison, N.B., Steinfield, C.: Changes in use and perception of facebook. In: Proceedings of the 2008 ACM Conference on Computer Supported Cooperative Work, pp. 721–730. ACM (2008)
22. Bonneau, J., Preibusch, S.: The privacy jungle: on the market for data protection in social networks. In: Moore, T., Pym, D., Ioannidis, C. (eds.) Economics of Information Security and Privacy, pp. 121–167. Springer, Boston (2010)
23. Gross, R., Acquisti, A.: Information revelation and privacy in online social networks. In: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, pp. 71–80. ACM (2005)
24. Lewis, K., Kaufman, J., Christakis, N.: The taste for privacy: an analysis of college student privacy settings in an online social network. J. Comput. Mediated Commun. **14**(1), 79–100 (2008)
25. Forman, C., Ghose, A., Wiesenfeld, B.: Examining the relationship between reviews and sales: the role of reviewer identity disclosure in electronic markets. Inf. Syst. Res. **19**(3), 291–313 (2008)
26. Koroleva, K., Brecht, F., Goebel, L., Malinova, M.: Generation facebook-a cognitive calculus model of teenage user behavior on social network sites. In: Proceedings of AMCIS 2011 (2011)
27. Pempek, T.A., Yermolayeva, Y.A., Calvert, S.L.: College students' social networking experiences on facebook. J. Appl. Dev. Psychol. **30**(3), 227–238 (2009)
28. Granovetter, M.: The strength of weak ties: a network theory revisited. Sociol. Theory **1**(1), 201–233 (1983)
29. Burke, M., Marlow, C., Lento, T.: Feed me: motivating newcomer contribution in social network sites. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 945–954. ACM (2009)
30. Shah, R.C., Sandvig, C.: Software defaults as de facto regulation the case of the wireless internet. Inf. Commun. Soc. **11**(1), 25–46 (2008)
31. Goldstein, D.G., Johnson, E.J., Herrmann, A., Heitmann, M.: Nudge your customers toward better choices. Harvard Bus. Rev. **86**(12), 99–105 (2008)
32. Johnson, E.J., Goldstein, D.: Do defaults save lives? Sci. New York then Washington **302**, 1338–1339 (2003)
33. Jin, L.: Improving response rates in web surveys with default setting the effects of default on web survey participation and permission. Int. J. Mark. Res. **53**(1), 75–94 (2011)
34. Kahneman, D., Knetsch, J.L., Thaler, R.H.: Anomalies: the endowment effect, loss aversion, and status quo bias. J. Econ. Perspect. **5**, 193–206 (1991)
35. Dhar, R., Nowlis, S.M.: The effect of time pressure on consumer choice deferral. J. Consum. Res. **25**(4), 369–384 (1999)
36. Iyengar, S.S., Lepper, M.R.: When choice is demotivating: can one desire too much of a good thing? J. Pers. Soc. Psychol. **79**(6), 995 (2000)
37. Kesan, J.P., Shah, R.C.: Setting software defaults: perspectives from law, computer science and behavioral economics. Notre Dame L. Rev. **82**, 583 (2006)
38. Hargittai, E., et al.: Facebook privacy settings: who cares? First Monday **15**(8) (2010). http://firstmonday.org/article/view/3086/2589

39. Stern, T., Kumar, N.: Improving privacy settings control in online social networks with a wheel interface. J. Assoc. Inf. Sci. Technol. **65**(3), 524–538 (2014)
40. Faul, F., Erdfelder, E., Lang, A.-G., Buchner, A.: G* power 3: a flexible statistical power analysis program for the social, behavioral, and biomedical sciences. Behav. Res. Meth. **39**(2), 175–191 (2007)
41. Field, A.: Discovering Statistics using IBM SPSS Statistics. Sage, London (2013)
42. Scheirer, C.J., Ray, W.S., Hare, N.: The analysis of ranked data derived from completely randomized factorial designs. Biometrics **32**, 429–434 (1976)
43. Krasnova, H., Hildebrand, T., Guenther, O., Kovrigin, A., Nowobilska, A.: Why participate in an online social network? an empirical analysis (2008)
44. Archambault, A., Grudin, J.: A longitudinal study of facebook, linkedin, and twitter use. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 2741–2750. ACM (2012)
45. Quinn, D., Chen, L., Mulvenna, M.: Does age make a difference in the behaviour of online social network users? In: 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing (iThings/CPSCom), pp. 266–272. IEEE (2011)
46. Richter, A., Riemer, K.: Corporate social networking sites-modes of use and appropriation through co-evolution. In: ACIS 2009 Proceedings (2009)
47. DiMicco, J.M., Geyer, W., Millen, D.R., Dugan, C., Brownholtz, B.: People sensemaking and relationship building on an enterprise social network site. In: 42nd Hawaii International Conference on System Sciences, HICSS 2009, pp. 1–10. IEEE (2009)