C4PS - Helping Facebookers Manage their Privacy Settings

Thomas Paul, Martin Stopczynski, Daniel Puscher, Melanie Volkamer, Thorsten Strufe

CASED, Technische Universität Darmstadt

Abstract

The ever increasing popularity of Online Social Networks has left a wealth of personal data on the web, accessible for broad and automatic retrieval. Protection from undesired recipients and harvesting by crawlers is implemented by access control, manually configured by the user in his privacy settings. Privacy unfriendly default settings and the user unfriendly privacy setting interfaces cause an unnoticed over-sharing. We propose *C4PS - Colors for Privacy Settings,* a concept for future privacy setting interfaces. We developed a mockup for privacy settings in Facebook as a proof of concept, applying color coding for different privacy visibilities, providing easy access to the privacy settings, and generally following common, well known practices. We evaluated this mockup in a lab study and show in the results that the new approach increases the usability significantly. Based on the results we provide a Firefox plug-in implementing C4PS for the new Facebook interface.

1 Introduction

Over 850 million users allegedly share personal information, private photos, videos, opinions and discussions on Facebook. The shared personal information include their age, gender, sexual preferences, taste and hobbies. All this data stored in Facebook or any other Online Social Network (OSN) can be linked to the relating individual by their real names published in their profiles.

Access to all this information is controlled by the OSN service provider, based on the user's privacy settings. Several studies have shown that despite increasing awareness [1,7], users due to the intricacy of the task are incapable of configuring their intended settings, and indeed do not understand their activities' implications [23]. However, the fact that Facebook and other OSNs have modified the default privacy settings to be more and more open with each update, makes it very important that users can easily grasp and change their privacy settings.

Consequences of this situation span unintended over sharing, and more serious threats, arising as scraping and harvesting [21,25], automated social engineering [5,6], social phishing [15] as well as various further attacks. In face of this perilous incomprehensibility, [17,10] go as far as proposing to abandon

©2013 Springer. The final publication is available at http://link.springer.com/chapter/10.1007%2F978-3-642-35386-4_15.

access control entirely and applying usage control and data ownership instead. However, this approach is not feasible with current technology, and the reasoning is in stark contrast to several other studies [3,22].

Previous research concordantly argues that privacy enhancing technologies, including distributed and secure data storage are important for OSN. Yet, it can only improve the situation if the users are actually able to properly configure their privacy settings. Furthermore, there is consent that this can only be ensured by increasing intelligibility of current privacy controls.

To this end we propose *C4PS - Colors for Privacy Settings*, a novel concept for privacy settings and their representation. *C4PS* aims at minimizing the cognitive overhead of the authorization task, based on three foundations:

- Color coding of authorization settings with immediate feedback upon change,
- one-click configuration based on proximity of data and respective controls,
- group-based access control through aggregated configuration, and easy group management based on drag-and-drop.

While we implemented and tested *C4PS* as a proof of concept for Facebook, the idea is generally applicable to any OSN, or other web pages with privacy settings. We started with a *C4PS* mockup for the Facebook interface early 2011 to evaluate, if *C4PS* indeed simplifies the authorization task and performed a lab user study. The results

- indicate that modifying and inspecting the privacy settings is significantly easier and more efficient when applying *C4PS* and
- confirm previous studies showing that even users who consider themselves proficient with the Facebook site are unable to correctly perform precise privacy settings.

Based on the results of the study we provide a Firefox plug-in applying *C4PS* to the modified Facebook interface after the introduction of the *Timeline* for download.

The rest of this paper is organized as follows: Putting *C4PS* into perspective, we give an overview of related work in Section 2. We present the rationale concept and design of *C4PS* in Section 3. The methodology of our user study is described in Section 4 and its results in Section 5. We conclude the paper with a summary and future work in Section 6.

2 Related Work

Improving privacy in OSNs is a very widely discussed issue in current literature [19,18]. One research area covers the confidentiality concerns towards OSN providers as one single entity that needs to be trusted. Approaches to resolve this vulnerability include several proposals to apply encryption and/or decentralized storage of user data. The range starts with cutting the profile in centralized OSNs into atomic parts, encrypting each part separately and distributing keys to authorized recipients only [14]. It ends with completely distributed peer to peer

(p2p) OSNs like PeerSoN [9], DESCENT [16] or Safebook [11]. These approaches help to assure users' privacy needs with technical support by architectural means or applying crypto, assuming that users are aware of the consequences of publishing personal data, as well as able and willing to commit themselves in subject of privacy. These approaches still require the data owners to grant access to authorized users to selected data.

Several studies and experiences have shown that the ability to understand and modify privacy settings is generally missing [1,7,3,2]. One class of proposals attempts to decrease the frequency of explicit acts of authorization by applying methods from machine learning to pre-configure the overall settings [13]. To "detect and report unintended information loss" [4] supports users, too. Explicit authorization however is still needed to train the recommender and to fine tune the settings.

Further approaches have tried to make it easier for users to manually grasp their current privacy settings. [12] use an interface, based on Venn diagrams. But they don't meet our design Principle 2 to use well known pattern and don't help users in managing their groups. [22] present a privacy setting interface which helps users of Facebook to understand the effect of their changes by providing an audience view. Users are presented their own profile in the way that a single potential other recipient would see it. The limitation of this approach is that users are not efficiently able to figure out the visibility of profile items to whole groups of friends, nor does it aid the users in granting authorization. Mazzia et al. addressed this limitation in [24] by creating the "PViz Comprehension Tool" which is able to illustrate privacy settings by color (from light to dark), "based on the user's privacy selection for a selected profile item". These improvements alleviate to build and verify the user's mental model of the interface by showing the effects of the conducted adjustments.

Our approach in contrast leads to a new mental model in terms of OSN access control. It is based on color coding, which is well known from other areas of the user's environment. Based on daily experience, users understand the effects of their adjustments at our privacy setting interface with a minimum amount of effort. Combined with single click changes we seriously reduced the obstacle of configuring access control rule sets.

3 C4PS - Improved Interface

To improve the usability of privacy settings, we developed a corresponding *C4PS* - overlay for Facebook.

3.1 Design Principles

The concept of *C4PS* is based on four main principles. The first three cover usability aspects according to ISO 9241, and the last one the applicability of the interface.

P1 - Little Effort: To ensure high accuracy when working with the interface, the user shall be able to check or change his privacy setting with as little effort (easy and fast) as possible (inspired by ISO 9241-11 – effectiveness and efficiency; and [20]).

P2 - Applying Common Practices: To minimize the learning effort while becoming accustomed to our interface, commonly accepted and well-known usability patterns shall be used to support users – like colors, drag and drop, tooltips or graying out inactive elements (inspired by ISO 9241-10 – conformity with user expectations).

P3 - Direct Success Control: To avoid gaps between intended and actually performed adjustments (as shown in [23]), results of modifications to the privacy settings shall be displayed and visible instantly (inspired by ISO 9241-10 – self descriptiveness).

P4 - Applicability: To cause the least possible cognitive overhead for accustomed users and to stay independent of Facebook, *C4PS* needs to allow for direct integration into the existing web pages.

Based on these four principles, we developed concepts for *C4PS*, identifying a need for new functionality for both the main privacy settings as well as the group management.

3.2 C4PS Privacy Settings

Regarding the main privacy setting functionality we highlight each attribute in the profile by a particular color, depending on the group of people who are granted access. We also enable the user to change the accessibility with just one click, support the group selection with tooltips, make this privacy settings mode easily accessible, and provide very brief instructions. In addition, the privacy settings mode provides a button to check how others see the profile. These concepts are explained in detail in this subsection.

Color Coding: The colors used are guided by the well-known traffic light colors (*P2*). Blue was added to represent custom settings. The corresponding color definition is:

- *Red:* Visible to nobody
- *Blue:* Visible to selected friends
- *Yellow:* Visible to all friends
- *Green* Visible to everyone

All privacy settings are visualized by our color scheme in the *C4PS* privacy setting mode (*P4*), so that an attribute's visibility can be directly derived from its coloring (cmp. Fig. 1).

Easy To Modify Setting for Single Attributes:

The user can change the privacy setting for a specific attribute by simply clicking the buttons on the edge of the row on the right side (*P1*). The color of the buttons shows the visibility that will be set for the entry by clicking on it (e.g. in Fig. 1). The settings are changed immediately (*P3*), which is reflected

directly by a color change of the attribute's cell. If the user chooses "selected friends" (blue), a window opens in which friends or groups are granted access to the mentioned attribute. *Tooltip:*

To further increase the usability, tooltips indicate the setting corresponding to the color for each button (*P2*). Tooltips are shown when the mouse hovers over the button (cmp. Fig. 1).

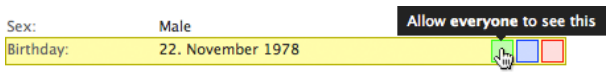

Fig. 1. Color coding for one attribute - birthday

Easy Access to Privacy Settings: C4PS integrates in the mockup a new button under the profile picture to enter the *C4PS* privacy settings page This button is visible on each FB page and thus the *C4PS* privacy settings page is easy to access (*P1*). After switching to the privacy editing mode and editing the privacy settings, the user can exit this mode by clicking a button labeled "Stop editing privacy settings" at the same place. In the improved version we enabled the visibility of color coding instantly without entering any privacy settings mode.

Information on Top of the Page: According to common practice (*P2*), general information about the color visualization and the meaning of each color are provided on top of the page in the editing mode.

Checking How Others See Their Own Profile: The privacy settings mode provides a button at the top of the page 'How others see your profile' , which offers a simple visualization to check how selected other people - including friends - see the profile (*P1*).

Application to Photo Albums: The privacy settings for photo albums can be checked and modified with the same color mechanism. When visiting the Facebook "photos" tab, an overview of all photo albums of the user is displayed, as in the original Facebook interface. However, there is an additional button labeled "Edit Privacy Settings" (cmp. Fig. 2).

This button again activates the *C4PS* privacy editing mode. Here, the photo album elements are highlighted with a color indicating the privacy setting (cmp. Fig. 3). Additionally, three colored buttons are shown on every item and allow to change the privacy setting as described before. Clicking on the colored buttons changes the privacy setting for the entire album, while individual restrictions, set to single photos, remain unchanged. To change the privacy settings of a single photo the user can open the photo album, in which the colored privacy buttons are placed under each photo.

With *C4PS*, checking and modifying privacy settings in Facebook takes a minimum of two steps:

1. Accessing the *C4PS* privacy settings main page by clicking on "Edit Privacy Settings" (no longer required in the improved version).

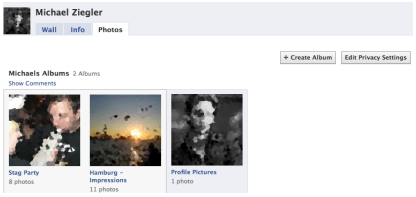

Fig. 2. Photo albums without privacy settings

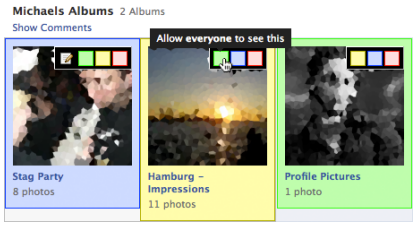

Fig. 3. C4PS interface - photo albums

2a To inspect the current settings for the profile entry, the user only needs to properly interpret the color. In case of custom settings a third step is required.
2b To change the setting of any attribute, the user can simply click on the button colored accordingly.

4 User Study

To evaluate *C4PS*, we conducted an extensive, controlled lab study. We aimed at validating the following four hypotheses:

H1 *C4PS* makes it easier and faster to find out to whom a particular attribute is visible.
H2 Using *C4PS*, testing how the complete profile is presented to another user is easier and faster.
H3 Setting the visibility of attributes is easier and faster using *C4PS*.
H4 The group management can be handled easier and faster using *C4PS*.

These four are intended to cover all aspects that may concern users aiming to adjust their privacy settings. In addition, we were interested in the feedback about the concrete ideas implemented in *C4PS* to further improve it.

We decided to run a lab study because this enabled us to measure time and clicks while the participants solved some tasks with both interfaces - the improved one and the original one. Correspondingly, the participants were asked to use a lab PC and a Facebook profile we created, to set a controlled environment and without warring the user to expose his own profile.

4.1 Course of Action

The study contained the following phases:

All tasks had to be solved in this particular order while it was not required to start from the main page after login. This course of action is more realistic, as users usually want to check or edit the privacy setting for more than a single attribute.

Nr.	Action
1.	OSN questionnaire[1] (on paper) containing eleven questions regarding the use of OSN in order to estimate the prior knowledge of the test person.
2.	First practical part, during which several tasks have to be solved with one of the interfaces. Note, to prevent a possible learning effect due to the first use of one of the two interfaces, the order of presentation of the two interfaces was alternated for each test person. The answers were written down (on paper).
3.	"System Usability Scale" (SUS) questionnaire (on paper) as introduced by Brooke [8]. It allows measurements concerning effectiveness, efficiency and user satisfaction, and due to its generality is applicable to various types of systems.
4.	Second practical part
5.	SUS questionnaire was applied to the second interface.
6.	Usability questionnaire (on paper) containing 15 questions regarding the usability of the new interface and a field for general comments.
7.	Demographic questions (on paper) concerning age, gender, and profession.

Nr.	In the practical part of the study, we asked the test persons to:
1.	Find out to which users or groups the birthday (Task 1) / hometown (Task 2) / relationship status (Task 3) / a particular photo album was visible (Task 4)
2.	Find out which attributes were visible for a specific friend (Task 5)
3.	Create a group "best friends" (Task 6)
4.	Add two particular friends and the group "class mates" to the group "best friends" (Task 7)
5.	Adjust the privacy settings of five attributes - mobile phone number to only two specific friends (Task 8.1) / interests to all (Task 8.2) / hometown to only one specific group (Task 8.3) / relationship to no one (Task 8.4) / religious and political views to all friends (Task 8.5)
6.	Adjust the privacy settings of one selected photo album, granting access to a specific group, except a single particular friend, being part of the group (Task 9).

4.2 Evaluation Criteria

The following information was deduced from the screencast:

- *Time:* Time a test person needs to perform a task
- *Hits:* Number of clicks a user needs to complete a task
- *Precision:* The task-solving precision of a study participant. It is only distinguished between the values 1 (task solved completely and correctly) and 0 (failure to precisely solve the task).

The measurement of time and clicks for a task was performed manually. The first goal-directed mouse movement was taken as starting point for the measurement of a task. The end of the measurement was chosen to be the successful or failed completion of a task, or the user canceling the task. We used the time frame without mouse movement before a new task was started as an indicator for canceling. We did not count clicks incidentally placed beyond any button or link as well as multiple clicks on a button or link to start a function (while waiting

for the website to respond). This should preserve the comparability of values. All other clicks to perform a task were counted. This includes clicks on scroll bars, selecting text or clicking into input forms. The time and clicks between tasks was stripped.

To evaluate our hypotheses, we measure both the time and clicks it takes to solve a task to evaluate if a system is *easier and faster*, and we consider the precision of a solution as its success. The usability questions from the SUS questionnaire, Attrakdiff(tm) questionnaire, and our final own usability questionnaire additionally are taken into account to gauge intelligibility and acceptance of *C4PS*.

4.3 Sample Description

Recruiting was done in lectures and via email lists. The information provided to the participants was that a new interface for the privacy settings in Facebook would be tested. Participants were rewarded with sweets.

The study was performed with 40 students, aged between 20 to 32 years. All were members of at least one OSN, except for three participants. 57,5% access their OSN profile(s) at least once a day and 25% even several times a day. Nearly two thirds of the test persons are Facebook users. Almost all study participants (90%) have already been in touch with the privacy settings of their OSN provider. However, many of them consider these settings to be confusing (57,5%). 15% of the participants were very concerned about their privacy settings and stated that they modify or check them every month. The rest did it less often. 30% did not change the privacy settings, after they have been set up once. The possibility to create lists or groups of friends, was only used by 25% of the participants and the possibility to set certain rights for groups or for individual friends was used by 37,5%. 62,5% of the participants stated that they are aware of the visibility of their profile's attributes to other network members.

5 Results

We first provide the results of the study regarding success rate and efficiency (Subsection 5.1). Afterwards, we discuss the feedback regarding the three usability questionnaires (Subsection 5.2 and 5.3). We show that the four hypotheses can all be confirmed in each category according to the evaluation criteria defined in Subsection 4.2. Based on these results we provide some ideas for further improvements.

5.1 Success Rates and Efficiency Analysis

In this subsection we show that the four hypotheses hold regarding the success rates, the time needed, and the number of clicks needed to complete the corresponding tasks.

Success Rates. The overall success rate for all tasks and all participants in the new interface is 91% while it is only 68% for the original Facebook interface. As shown in Figure 4, the success rate for the new interface is higher than the one for the original interface in almost all tasks. Only for task 3, the original Facebook interface performed better. Here, subjects were asked to list the friends or groups who have access to the attribute "Relationship Status". Unfortunately the participants wrote down the privacy setting "selected friends" while we expected them to read out the actual list of friends who have access. In most cases the participant did not click on the blue button in order to get this information but only wrote down the tooltip text (selected friends) that was revealed when hovering over the button. Some other participants did not write down all groups having access to this attribute or the wrong ones. According to our definition both cases were interpreted as wrong answers.

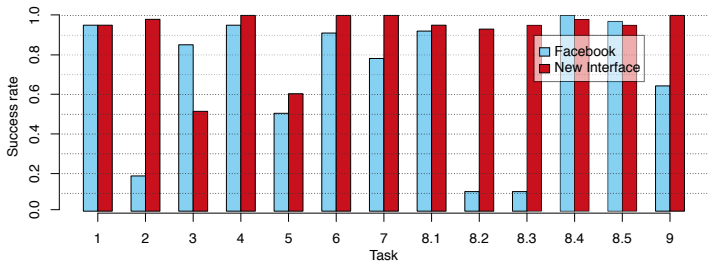

Fig. 4. Success rate per task

The biggest difference was measured at task 2 (visibility of the field "current city and hometown"). Only 17,5% of the participants solved this task correctly with the original interface, while all but one participant succeeded using the new interface. One reason for this is that this attribute is placed on Facebook in the slightly hidden "Connecting on Facebook"-section and not on the main privacy settings page. In addition, many participants wrote down the value of the incorrect attribute "Contact information", which was displayed on the main privacy settings page on Facebook. The difference between both interfaces again is very large for Task 8.2 and 8.3, for a similar reason, and the participants hence changed the wrong attribute. For task 8.3, participants changed the field "Contact information" instead of "hometown" while for task 8.3 the incorrect attribute "Interested in" was changed, instead of "Interests". The latter in this case represents the gender the user is interested in rather than the intended interest in his activities like sport, films, music or other.

Efficiency Analysis. The efficiency analysis with respect to time and clicks below compares only tasks 5 to 9, since in these tasks the participants actually had to change settings, rather than interpreting the current configuration.

Therefore, for these first four tasks it is not clear from the videos when a participant completed a task and started the next.

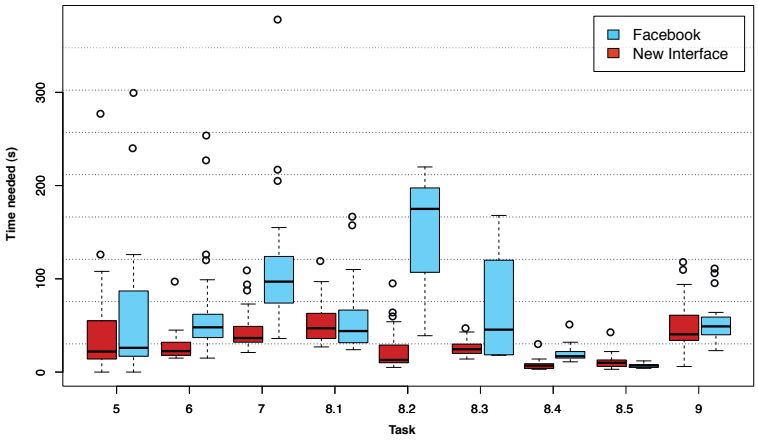

Fig. 5. Required time (per task)

The minimum number of clicks to properly execute all four Tasks (1-4) using *C4PS* is one click on "Edit Privacy Settings" from the main page, then interpreting the privacy settings for the first two requested attributes. In the case of task 3, a further click was required, as the displayed privacy level "selected friends" was not the proper answer, but it was necessary to interpret which selected friends were granted access by clicking on the blue button. Thus, one click was necessary to open the dialog, and another one to close it. Similarly, it was required to click on the photo album settings to discover this information. The minimum number of clicks in *C4PS* thus amounted to 4. The minimum number of clicks to execute these tasks properly in Facebook amounted to 8.

Time needed: Most tasks were completed faster when using *C4PS*, as shown in Fig. 5. Especially when adjusting privacy settings that are in the "Connecting on Facebook"-category and while creating groups. The test users on average need more than twice as much time to solve the tasks using the Facebook interface, as compared to *C4PS*. Fig. 5 also shows that the variance using *C4PS* is much lower for most tasks, indicating that all users achieved approximately the same efficiency.

Clicks needed: Considering the number of clicks (Fig. 6), the results are very similar to those from the time measurement. Most tasks can be solved with much fewer clicks using *C4PS*, and the variance is very low. The participants generally needed nearly three times more clicks to complete the task using the original interface. Note, that it can be assumed that a much greater deviation would have been achieved, if all privacy setting tasks had to be performed separately starting from the main menu. Using the Facebook interface, the user would have needed to perform at least three additional clicks to get to the settings menu, compared to a single click that is necessary using *C4PS*.

Comparing users with and without Facebook Accounts. The test persons who already use Facebook had an advantage when solving the tasks, because they

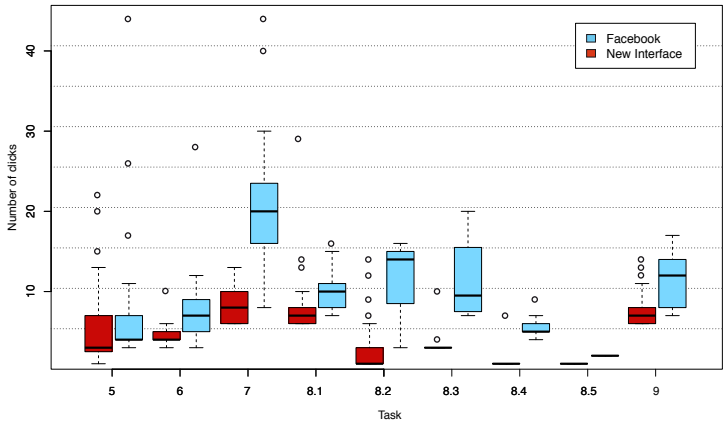

Fig. 6. Required number of clicks (per task)

already knew the look and feel of the Facebook interface, or even the concerning privacy settings. However, even these participants achieved better success rates with *C4PS*, even if they could be considered Facebook experts for using it every day. In numbers, the success rate of Facebook experts for the tasks on Facebook was 73% compared to a success rate of 94% when using *C4PS*. Subjects who were not considered Facebook experts only reached a success rate of 60% for the task when using the original interface, rising to a success rate of 86% when using *C4PS*.

Almost all tasks have been solved better by participants that are Facebook users (in both interfaces). Solving the task on Facebook, the experts needed 1.65 less clicks on average. When using *C4PS*, the disparity between experts and normal users was smaller. The experts in this case completed the task with 0.89 less clicks. Measuring the time for completing tasks, the experts performed 1.76 times faster using Facebook. Using *C4PS*, however, the experts were only 0.75 times faster. This disparity shows an additional improvement of the usability of the systems, and the subjects who had not used Facebook before had a much harder time to cope with the original interface at all.

The results for all three criteria show that even users who consider themselves proficient with Facebook are unable to correctly perform precise and efficient privacy settings.

5.2 SUS - System Usability Scale

In this subsection we show that *C4PS* performs better regarding SUS.

The average System Usability Scale (SUS) [8] value for our interface (all users) has been evaluated to 82.6. The maximum possible SUS value of 100 was achieved at maximum, and the worst rating of the interface was valued at 37.5.

Comparing this with Facebook, the users rated the interface with an average SUS value of 35. The maximum value was 75 and the minimum was 5. Referring to A. Bangor et al. who analyzed the results of 2324 studies with SUS in the last ten years [8], acceptable products have a SUS-score of over 70. Better products start at the high 70s and end in the upper 80s range. Only truly excellent products have a score above 90. Products with scores less than 50 should be cause for significant concern and are judged to be unacceptable. Due to this scale, the usage of our interface is very good while Facebook itself reaches numbers below those for acceptable products.

5.3 Concept Evaluation

At the end of the study, we asked the study participants what they like and do not like as well as what they would improve. The results of this questionnaire are discussed in this Subsection. They show that *C4PS* also performs better regarding these interface specific usability questions, and that people like the general concepts.

57,5% of the participants rated the original Facebook privacy setting mechanisms as confusing (the worst level on a scale of 4 possibilities) and only one stated that it is very clearly arranged (the best level). 87,5% of the participants stated that *C4PS* improved the situation a lot (maximum improvement of a scale of 4 options). On a scale with 4 options 50% rated the visualization with colors as very good, 47,5% with good and the rest with level 3 while no one selected level four. The question whether the color coding is well-defined was agreed by 31 (77,5%) of the participants.

Only 20% of the participants answered that they cope 'very well' or 'well' with the original interfaces for group management while 97,5% of the participants made this statement for the new interface. The question regarding the usability of the privacy setting mechanisms was answered with 'very good' by 5% of the participants for the original Facebook interfaces and by 47,5% for the new interfaces while 22,5% (FB) and 50% (new interface) stated that these mechanisms in the corresponding interfaces provide a 'good' usability.

There were also two fields to provide comments. In the first one we asked the participants what they liked most about the interface. Almost everyone mentioned the colors while only a few also mentioned the group management. People stated for instance that the privacy settings are 'easy', 'clearly arranged', 'directly accessible', 'easy to find', 'easy to use', 'everything is on one page', 'less clicks', 'quick', 'applicable for more attributes' and 'clear what to do'. In the second field we asked them to propose further improvements. Comments mainly addressed the group management and the profile preview in general and for the case that particular friends have the right to access this attribute. Some remarks were made regarding the colors - including only three colors, changing colors, self-defined colors; and also the fact that the order of the colored buttons in a row should stay the same.

6 Conclusion and Future Work

This paper deals with access authorization in Online Social Networks, and the specific case of Facebook. Even though users publish highly personal data on such sites, several studies have shown that they are incapable of configuring their privacy settings correctly. The direct consequence is unwanted over-sharing of highly personal information by the users, which allows for various attacks, including information harvesting and various types of social engineering.

To increase the intelligibility of the authorization controls, we have proposed, evaluated, and implemented *C4PS – Colors for Privacy Settings*. *C4PS* introduces a new mental model for the privacy settings, and has been designed as simple and intuitive as possible, to minimize the cognitive overhead of the authorization task. It is based on the foundations of color coding, simple, one-click configuration, and group-based access control, including a simplified group management interface. We initially implemented *C4PS* as a mockup for controlled lab studies.

Evaluating *C4PS* in an extensive, controlled user study demonstrated two main insights:

1. *C4PS* greatly aids the authorization steps – it not only enables the user to grant exactly the desired authorization, but additionally helps the user comprehend their authorization activities and current settings.
2. Even users that are convinced of their expertise using Facebook are unable to employ the existing privacy controls correctly and efficiently, and are unable to precisely configure their profile according to the desired authorization.

Both interface and privacy configuration of Facebook have changed during the course of this study. The presentation of the profiles has changed entirely, and following Google+, the privacy settings have been made seemingly simpler to use. The service increasingly encourages to organize the friends in groups, to facilitate the authorization step. The interface additionally introduced an icon to hide items from the timeline. This control is not implemented for posts to other users' walls, though, and no enhancements have been made to help comprehending current settings, and the consequences of applied authorization changes. We hence adapted *C4PS* to Facebook Timeline and implemented it in a Firefox plugin, which is available for download from our web site.

C4PS being a concept of general applicability, we are aiming at applying it to other social networking services, like for instance Google+, Twitter and Foursquare, in future work. We are additionally aiming at analyzing the applicability of the main principles of *C4PS* to present other complex settings, configurations, and further properties of online services, thus making them easier to grasp and to handle.

References

1. Acquisti, A., and Gross, R. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In *PET* (2006).

2. Antón, A. I., Earp, J. B., and Young, J. D. How Internet Users' Privacy Concerns Have Evolved since 2002. *IEEE Security & Privacy Magazine 8*, 1 (Jan. 2010), 21–27.
3. Balfanz, D., et al. In Search of Usable Security. *IEEE Security & Privacy* (2004).
4. Becker, J., and Chen, H. Measuring privacy risk in online social networks.
5. Bilge, L., Strufe, T., Balzarotti, D., and Kirda, E. All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks. In *WWW* (2009).
6. Boshmar, Y., et al. The Socialbot Network: When Bots Socialize for Fame and Money. In *ACSAC* (2011).
7. Boyd, D., and Hargittai, E. Facebook privacy settings: Who cares? First Monday [Online].
8. Brooke, J. SUS - A quick and dirty usability scale. Usability evaluation in industry, 1996.
9. Buchegger, S., et al. PeerSoN: P2P Social Networking - Early Experiences and Insights. In *SNS* (2009).
10. Castelluccia, C., and Kafaar, D. Owner-Centric Networking: Toward a Data Pollution-Free Internet . In *SAINT* (2010).
11. Cutillo, L.-A., Molva, R., and Strufe, T. Safebook: a privacy preserving online social network leveraging on real-life trust. *IEEE Communications Magazine* (2009).
12. Egelman, S., Oates, A., and Krishnamurthi, S. Oops, i did it again: mitigating repeated access control errors on facebook. CHI '11.
13. Fang, L., Kim, H., LeFevre, K., and Tami, A. A Privacy Recommendation Wizard for Users of Social Networking Sites. In *CCS* (2010).
14. Guha, S., Tang, K., and Francis, P. NOYB: Privacy in Online Social Networks. In *WOSP* (2008).
15. Jagatic, T. N., Johnson, N. A., Jakobsson, M., and Menczer, F. Social Phishing. *Commun. ACM* (2007).
16. Jahid, S., Nilizadeh, S., Mittal, P., Borisov, N., and Kapadia, A. DECENT: A Decentralized Architecture for Enforcing Privacy in Online Social Networks.
17. Kagal, L., and Abelson, H. Access Control is an Inadequate Framework for Privacy Protection. In *W3C Privacy* (2010).
18. King, J., Lampinen, A., and Smolen, A. Privacy : Is There An App for That ? In *Symposium on Usable Privacy and Security (SOUPS)* (2011).
19. Krishnamurthy, B., and Naryshkin, K. Privacy leakage vs. Protection measures: the growing disconnect. *W2SP, May* (2011).
20. Krug, S. *Don't Make Me Think: A Common Sense Approach to the Web (2nd Edition)*. New Riders Publishing, 2005.
21. Lindamood, J., et al. Inferring Private Information Using Social Network Data. In *WWW* (2009).
22. Lipford, H. R., Besmer, A., and Watson, J. Understanding Privacy Settings in Facebook with an Audience View. In *UPSEC* (2008).
23. Madejski, M., Johnson, M., and Bellovin, S. The Failure of Online Social Network Privacy Settings. Tech. rep., Columbia University, 2011.
24. Mazzia, A., LeFevre, K., and Adar, E. The pviz comprehension tool for social network privacy settings. Tech. rep., University of Michigan, 2011.
25. Strufe, T. Profile Popularity in a Business-oriented Online Social Network. In *EuroSys/SNS* (2010).