

# C4PS - Colors for Privacy Settings

Thomas Paul, Martin Stopczynski, Daniel Puscher, Melanie Volkamer, Thorsten Strufe  
 CASED, Technische Universität Darmstadt  
 Darmstadt, Germany  
 {firstname.lastname}@cased.de

## ABSTRACT

The ever increasing popularity of Facebook and other Online Social Networks has left a wealth of personal as well as private data on the web, aggregated and readily accessible for broad and automatic retrieval. Protection from both undesired recipients and harvesting by crawlers is implemented by access control, manually configured by the user and owner of the data. Several studies demonstrate that default settings cause an unnoticed over-sharing and that users have trouble understanding and configuring adequate privacy settings. We developed an improved interface for privacy settings in Facebook by mainly applying color coding for different groups, providing easy access to the privacy settings, and applying the principle of common practices. Using a lab study, we show that the new approach increases the usability significantly.

## Categories and Subject Descriptors

K.4.1 [Computers & Society]: Policy Issues—*Privacy*

## General Terms

Security, Design

## Keywords

Access Control, Privacy, Online Social Networks

## 1. INTRODUCTION

Over 800 mio. users allegedly share private photos, videos, opinions and discussions on Facebook, today. Their content consists of personal information including their age, gender, sexual preferences, taste and hobbies, directly linked to the relating individuals of sender or addressee by their real names published in their profiles.

Access to all this information is controlled by the service provider, Facebook in our case, with authorization granted using the interface for privacy settings of the site. Several studies have shown that despite increasing awareness [1, 4], users due to the intricacy of the task are incapable of configuring their intended settings, and indeed do not understand their activities' implications [8].

Consequences of this situation span unintended over sharing, and more serious threats, arising as scraping and har-

vesting [7, 9], automated social engineering [2, 3], social phishing [5] and various further attacks. Hence we propose *C4PS*, a novel design for the 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.

We have implemented *C4PS* for Facebook, which in general can be integrated into any Online Social Network (OSN) site or other web pages with privacy settings, both as a prototype and Firefox plugin. To evaluate, if *C4PS* indeed simplifies the privacy settings, we performed an extensive user study after. The results indicate that modifying and inspecting the privacy settings is significantly easier as well as more efficient when using *C4PS*. Furthermore, it confirms previous studies showing that even users who consider themselves proficient with the Facebook site are unable to correctly perform precise privacy settings.

The remainder of the paper describes our interface, the user study and the resulting outcomes of the user study.

## 2. INTERFACE

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 settings with as little effort (easy and fast) as possible (ISO 9241-11 – effectiveness and efficiency; [6]).

*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 (ISO 9241-10 – conformity with user expectations).

*P3 - Direct Success Control:* To avoid gaps between intended and actually performed adjustments (as shown in [8]), results of modifications to the privacy settings shall be displayed instantly (ISO 9241-10 – self descriptiveness).

*P4 - Applicability:* To cause the least possible cognitive overhead for accustomed users and to stay independent of

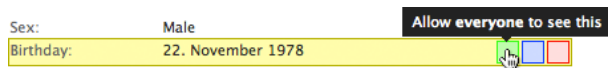
Facebook, *C4PS* needs to allow for direct integration into the existing web pages.

Inspired by these four principles, we highlight each attribute in the profile by a particular color, depending on the group of people who have access to this attribute. 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 your profile. These concepts are explained in detail in this subsection.

*Color Coding:* The colors used are guided by the well-known traffic light colors. 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, so that an attribute's visibility can be directly derived from its coloring (cmp. Fig. 1).



**Figure 1: Color coding for one attribute - birthday**

The user can change the privacy setting for a specific attribute by simply clicking the privacy setting for a specific attribute by simply clicking the privacy setting for a specific attribute by simply clicking the privacy setting for a specific attribute by simply clicking the privacy setting for a specific attribute on the right side. The color of the buttons shows the visibility that will be set for the entry by clicking on it (cmp. Fig. 1). The privacy settings for photo albums can be checked and modified in the same way.

### 3. USER STUDY

Based on a locally implemented showcase and a real Facebook profile, we performed a user study with 40 young adults, aged between 20 to 32 years. 37 were members of at least one OSN, 65% 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. The study was conducted by solving some tasks and answering a questionnaire, consisting of four sections:

1. General questions regarding the use of online social networks to estimate the participant's prior knowledge
2. a practical part where several tasks have to be solved with both interfaces
3. an evaluation and comparison possibility part of the two interfaces
4. acquisition of some demographical information like age, gender and profession.

The tasks of the practical part of the user study were designed to fit everyday needs like changing access policies for a given attribute like the birthday as well as more sophisticated tasks like creating groups. A second focus was put on checking the effects of the changes that were made. We specifically asked the test persons to:

- find out to which users or groups the birthday / hometown / relationship status / a photo album is visible
- find out which attributes are visible for a specific friend
- create a group "best friends"
- add the two friends and the group "class mates" to the group "best friends"
- adjust the privacy settings of some attributes and one photo album.

In order to compare the new interface with the interface currently used at Facebook, the tasks of the study have to be performed with both interfaces. For each task, several measurements were made:

- *Time:* Time it takes for a test person to perform a task.
- *Hits:* Counted number of clicks it takes a user 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 (task resolved only partially or not at all).

## 4. RESULTS

Our results showed that the usage of the new interface reduced the time and the number of clicks, which were needed to find the privacy settings and to effectively perform the tasks by the factors of 1.7 and 1.8. The most remarkable fact is that even Facebook experts are faster and more precise with the new interface, too.

During our study, the privacy-interface of Facebook was perceived as confusing by most subjects. The new interface was rated much better by 87% of the subjects. The representation of the privacy-settings by colors was rated as good or very good by all and the overall success rate to finish a tasks increased by 23%.

## 5. REFERENCES

- [1] A. Acquisti and R. Gross. Imagined communities: Awareness, information sharing, and privacy on the facebook. In *PET*, 2006.
- [2] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All your contacts are belong to us: Automated identity theft attacks on social networks. In *WWW*, 2009.
- [3] Y. Boshmar et al. The socialbot network: When bots socialize for fame and money. In *ACSAC*, 2011.
- [4] D. Boyd and E. Hargittai. Facebook privacy settings: Who cares? First Monday [Online], 2010.
- [5] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer. Social phishing. *Commun. ACM*, 2007.
- [6] S. Krug. *Don't Make Me Think: A Common Sense Approach to the Web (2nd Edition)*. New Riders Publishing, 2005.
- [7] J. Lindamood et al. Inferring private information using social network data. In *WWW*, 2009.
- [8] M. Madejski, M. Johnson, and S. Bellovin. The failure of online social network privacy settings. Technical report, Columbia University, 2011.
- [9] T. Strufe. Profile popularity in a business-oriented online social network. In *EuroSys/SNS*, 2010.