Helping John to Make Informed Decisions on Using Social Login

Farzaneh Karegar
Karlstad University
farzaneh.karegar@kau.se

Nina Gerber
Technische Universität Darmstadt
nina.gerber@secuso.org

Melanie Volkamer
Karlstad University and Technische Universität Darmstadt
melanie.volkamer@{kau.se,secuso.org}

Simone Fischer-Hübner
Karlstad University
simone.fischer-huebner@kau.se

ABSTRACT

Users make two privacy-related decisions when signing up for a new Service Provider (SP): (1) whether to use an existing Single Sign-On (SSO) account of an Identity Provider (IdP), or not, and (2) the information the IdP is allowed to share with the SP under specific conditions. From a privacy point of view, the use of existing social network-based SSO solutions (i.e. social login) is not recommended. This advice, however, comes at the expense of security, usability, and functionality. Thus, in principle, it should be up to the user to consider all advantages and disadvantages of using SSO and to consent to requested permissions, provided that she is well informed. Another issue is that existing social login sign-up interfaces are often not compliant with legal privacy requirements for informed consent and Privacy by Default. Accordingly, our research focuses on enabling informed decisions and consent in this context. To this end, we identified users' problems and usability issues from the literature and an expert cognitive walkthrough. We also elicited end user and legal privacy requirements for user interfaces (UIs) providing informed consent. This input was used to develop a tutorial to inform users on the pros and cons of sign-up methods and to design SSO sign-up UIs for privacy. A between-subject laboratory study with 80 participants was used to test both the tutorial and the UIs. We demonstrate an increase in the level to which users are informed when deciding and providing consent in the context of social login.

CCS CONCEPTS

• **Security and privacy** → *Social aspects of security and privacy*; *Privacy protections*; *Usability in security and privacy*;

KEYWORDS

Informed Decision, Usable Privacy, Privacy by Design, GDPR, Single Sign-on.

ACM Reference Format:
Farzaneh Karegar, Nina Gerber, Melanie Volkamer, and Simone Fischer-Hübner. 2018. Helping John to Make Informed Decisions on Using Social Login.

1 INTRODUCTION

Single Sign-On (SSO) solutions provided by social networks are broadly deployed nowadays. Facebook, Google, and Twitter are three top-English speaking services that also act as Identity Providers (IdPs) [27] enabling authentication to another Service Provider (SP), also known as a relying party. When signing up to websites offering a social login to sign up besides a manual option, users encounter two privacy-related decisions. First, they need to decide if they should sign up using the social login method, and secondly they need to decide if they want to consent to grant access permissions to the SP to sharing personal information from their social network profile, under specific conditions. Contrary to a manual sign-up[1] method for SPs, a social login relieves users of the need to recall many sets of credentials and it is less time consuming, as the personal information is forwarded directly from the IdP to the SP. However, the social network also becomes a single point of failure as without the network and the account one cannot sign in to the SP. Moreover, the social network also learns to which services and when its customers communicate; thus the SSO method enables increased user profiling. Further privacy issues result from the way that permissions to share personal information from the social network profile are granted to an SP. The current UIs for signing up with social login methods and for consenting to share information with unclearly displayed opt-out, instead of clear opt-in, choices make it difficult for users to conceive, notice and control what they share: e.g. previous studies show that participants were not aware of the information they consented to share or even that the service provider also had the right to access this information in future [4, 24]. Thus, users do not give their informed consent since, contrary to current practice, users should be fully informed as to what they are consenting when they use social login methods. Enabling an informed decision is a known problem in the privacy context [10] and a prerequisite for obtaining consent for data processing, which must be freely given, specific and informed, according to Art. 4 (11) of the EU General Data Protection Regulation (GDPR) [25]. An informed decision does not necessarily imply that people should select the most privacy-friendly method or disclose less personal information, even though this should be offered to the user as the default option, according to the Data Protection by Default principle postulated by Art. 25 GDPR. An informed decision means

[1] Sign-up: registration for the first time.

that the individual can decide based on insights into different sign-up methods, on the personal information about them that can be shared, with whom, and under which conditions.

The objective of our research presented here is to develop and evaluate the means to empower users to make informed decisions, in the context of the social login methods. To support users in deciding whether to use social logins, a tutorial was developed. Furthermore, to achieve informed consent to share personal information, new UI concepts based on 'Drag and Drop' and 'Question and Answer' were designed, developed and tested.

Tsormpatzoudi et al. [26] emphasize the importance of involving end-users as stakeholders in the Privacy by Design process, involving multiple disciplines including usability design, as the end users should ultimately profit from Privacy by Design. Also, Cavoukian stresses that the Privacy by Design principle *Respect for Privacy* extends to the need for UIs to be "human-centered, user-centric and user-friendly, so that informed privacy decision may be reliably exercised" [8]. For developing our UIs, we follow a Privacy by Design and human-centered approach involving end users as stakeholders by addressing end user-specific and legal privacy requirements from the beginning and throughout the UI development cycle.

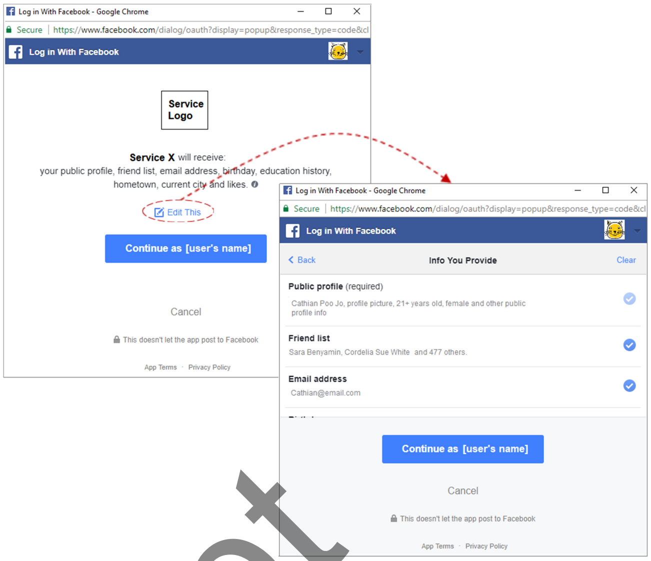
The remainder of this paper is structured as follows: First, users' misconceptions and problems identified in i) literature, ii) a cognitive walkthrough, and iii) a legal analysis, help us define design requirements to obtain informed decisions from users, and are presented in Section 2. Meeting those requirements resulted in i) general knowledge necessary to know about the concept in order to make an informed decision (transferred into a short tutorial in Section 3), and ii) effective new UIs to enable informed consent (Section 3). Both the tutorial and the UIs were developed in an iterative process and evaluated in a lab user study with 80 participants (Section 4). Results are discussed in Section 5 and 6. Section 7 discusses related work and Section 8 concludes the paper.

2 REQUIREMENTS

Firstly, to propose solutions to help users to make informed decisions, users' problems, misconceptions and usability problems of the current Facebook UIs are analysed. Then, relevant requirements to counter users' problems and to make better-informed decisions are elicited. To this end, a literature review, a legal analysis and an expert cognitive walkthrough (CW) on the current user interfaces of the Facebook SSO (see Figure 1) were conducted. The results are reported in this section.

2.1 Literature Review, CW and Derived Requirements

A CW is an expert review method in which interface experts imitate users, walking through a series of tasks [15]. We defined tasks with different types of users in mind to identify as many problems as possible. Two experts (authors of the paper) worked together on the current user interfaces of Facebook SSO to identify usability and potential users' problems. The detected problems (denoted with P#) from the CW and literature review [2, 4, 9, 20, 23, 24] help to elicit some requirements (denoted with R#) which can be categorised into three groups entailing sign-up/in, underlying process, and consent form related issues. For common findings and problems



Log in With Facebook - Google Chrome

Secure | https://www.facebook.com/dialog/oauth?display=popup&response_type=code&cl

Log in With Facebook

Service Logo

Service X will receive:
your public profile, friend list, email address, birthday, education history, hometown, current city and likes.

Edit This

Continue as [user's name]

Cancel

This doesn't let the app post to Facebook

App Terms · Privacy Policy

Log in With Facebook - Google Chrome

Secure | https://www.facebook.com/dialog/oauth?display=popup&response_type=code&cl

Log in With Facebook

< Back Info You Provide Clear

Public profile (required) ✓
Cathian Poo Jo, profile picture, 21+ years old, female and other public profile info

Friend list ✓
Sara Benyamin, Cordelia Sue White and 477 others.

Email address ✓
Cathian@email.com

Continue as [user's name]

Cancel

This doesn't let the app post to Facebook

App Terms · Privacy Policy

Figure 1: Facebook SSO authorization dialogues. The right one appears if the *Edit This* is clicked as indicated by the dashed line.

from the CW, literature review and the related elicited requirements we avoid redundancy and cite results in the literature review.

Sign-up/in Related Issues. The problems encountered from the CW and the elicited requirements in this group pertain to the decision a user should make regarding how to sign up for an SP.

P1: When a user wants to select between the sign-up methods, there is no source of information available for her by which she can gain knowledge about the properties of the methods and what happens if she selects them, i.e. the advantages, disadvantages, and the steps each method requires for sign-up process. **R1:** There is a need of a proper source of information for users who need more knowledge to decide on which method to use for sign-up.

P2: Depending on the current practices of the SP and the sign-up methods offered, different personal data may be requested by each method. However, before choosing the exact method, the type of personal data being requested by each method is not conveyed to users. **R2:** The personal data that each method requests should be communicated to users before the selection is made.

Process Related Issues. Being unaware of the underlying process (e.g. how the sign-up takes place) when using SSO systems caused problems and misconceptions for users, is reported in some literature [2, 23, 24]. The related requirements derived from the problems identified in literature and in the CW are listed below:

P3: Sun et al. reported [23, 24], that all of their participants expressed great concerns about IdP phishing attacks once they were informed of this issue; half the participants (51%), even when prompted, could not find any distinguishing features on a bogus Google login form. **R3:** The necessity to check for phishing attacks should be communicated to users.

P4: Results from the CW emphasise that users may get confused about new dialogues that open up showing the Facebook web page and then disappear again during the sign-up process. **R4:** The direction of movements and various steps should be clear for users during the entire process of sign-up.

P5: Sun et al.'s and Arianezhad's studies [2, 23, 24] clarify about participants' security misconceptions when they use SSO solutions. For example, among 19 participants including both experts and lay users, just four participants correctly answered that their IdP passwords were not learned by the SP [2]. **R5:** Users should not only be informed about the personal information that is shared with the SP but also that their credentials for the IdP are not shared.

Informed Consent Related Issues. The requirements categorised in this group relate to the lack of knowledge and meaningful transparency about the information an SP receives from an IdP, and under which conditions. In other words, there are problems related to improper consent forms.

P6: Results of different user studies show that there is a mismatch between participants' understanding and perception about the access rights they believe they grant and the access rights that they actually grant to SPs. Bauer et al. [4] show that participants have little insight into the level of access that SPs actually receive. 38% of participants erroneously believed that the SP could access the attribute just once. In addition, Sun et al. [24] report that most of their participants were uncertain about the types of data that they shared, and did not know that SPs can post messages back to the IdP on their behalf. **R6:** The users should be properly informed about the data they share with the IdP, for how long and the kind of access rights the IdP gets, based on their permissions.

P7: Over the years, interface designers trained users to repeatedly click dialogues to finish their primary tasks. Bauer et al. [4] report that participants' understanding of the information IdPs shared with SPs was based on preconceptions rather than the content of authorisation dialogues. In Egelman's study [9] participants also failed to notice the changes made to the dialogues, which is due to habituation. **R7:** Proper substitutions for current common integrated design solutions in authorisation dialogues, which are robust against habituation, should be considered.

P8: Robinson et al. [20] report that most participants did not realise that they were giving access to their personal information even if they had marked it with a privacy level other than public. **R8:** Users should be made aware of the irrelevance of privacy settings[2] and the shared information and proper design solutions should be considered to alert users when conflicts occur.

P9: The *public profile* information[3] which is always pre-selected to be shared by default, and is unchangeable, is not clearly defined as emerged in the CW. Users can have various interpretations of this item. **R9:** A clear description of the exact personal information being included in the *public profile* should be provided to users.

P10: [4] reports that the vast majority of their participants (84%) did not know that they could change their sharing decisions made previously; at the same time, almost half (48%) of the participants reported that the availability of an effective audit tool would cause them to use an IdP more often. **R10:** Users should be aware of the possibility to revoke granted permissions and how to do it.

P11: Results from the CW show that improper language and the size of objects used in the current Facebook authorisation interfaces are among the reasons why users' attention may be diverted and they finish the sign-up task before gaining proper knowledge of what is shared, and how. For example, the big button clicking on which means giving consent has an improper name: *Continue as [user's name]* and the size and colour dominate all the other objects on the screen. The problems also include the ambiguous link to change selected data (very small with an unrelated name), an uncommunicative sentence conveying the write access accompanied with an inappropriate lock icon, and the very small, hard-to-see links for privacy policies and terms of service of the SP (see Figure 1). **R11:** Language and size of objects should be designed to help users to not only finish the task but also to finish it while they are informed, and their privacy is not invaded.

2.2 Legal Requirements

As pointed out in [17], the legal privacy principles have Human-Computer Interaction (HCI) implications as they describe "mental processes and behavior of the end user that must be supported in order to adhere to the principle". In this section, we elicited legal requirements related to transparency and informed consent pursuant to the GDPR [25] and derived from Opinion 10/2004 of Art. 29 Data Protection Working Party [3] that has a potential impact on the design of authorisation dialogues. According to Art. 4 (11) GDPR, consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". This definition implies the following legal requirements are of special importance for our authorisation user interfaces:

R12: Consent should be given by a clear affirmative action (Art. 4 (11) GDPR). According to Recital 32 of the GDPR, the affirmative action could include ticking a box, choosing technical settings or other statements which clearly indicate the data subject's acceptance of the proposed processing of his or her personal data. Thus, implicit and *opt-out* consent and particularly *silence, pre-ticked boxes or inactivity* are presumed inadequate to confer consent. Opt-out choices for pre-selected data items that are not minimal, i.e. not needed for the purpose of the requested service, would also violate the Data Protection by Default principle of Art. 25 GDPR.

R13: Consent needs to be informed (Art. 4 (11) GDPR). Pursuant to Art. 13 (1) GDPR and stressed in Recital 42, when personal data are collected from a data subject (e.g. in the authorisation dialogue), the data subject should at least be made aware of the identity of the controller and the intended purposes of the processing of data. Furthermore, according to Art. 13 (2) GDPR, the controller shall provide the data subject with some further information to ensure fair and transparent processing. Such policy information includes but is not limited to information of recipients/categories of recipients, the period for which the personal data will be stored and data subject rights, including the right to withdraw consent at any time.

R14: Policy information to be provided pursuant to Art. 13 GDPR, needs to be given to the data subject in a concise, transparent, intelligible and easily accessible form (Art. 12 (1) GDPR). Making policy information more transparent and easily accessible, the Art. 29 Data Protection Working Party recommended in its Opinion 10/2004 [3] to provide policy information in a multi-layered format, where a short privacy notice on the top layer must offer individuals the core information, i.e. the identity of the controller and the data

[2] Controls available on many social networks and other websites that allow users to limit who can access their profile and what information visitors can see.

[3] Includes all information that is public by default (e.g. cover photo), made publicly available by users, or published publicly by others to Facebook, and is linked to a user's account.

processing purposes, and a clear indication must be given on how the individual can access the other layers presenting the additional policy information. Furthermore, according to the Data Protection by Default principle (Art. 25 GDPR), we derive:

R15: Only the minimal data needed for a service should be mandatory; other data items should be optional or voluntary.

Social login UIs of Facebook (1) do not comply with the legal requirements of the GDPR for informed consent. In regard to the requirement for a clear affirmative action (R12), even though users still have to click a button to finish the sign-up process and for providing consent, there is no clear instruction, since *Continue as [user's name]* button does not mean *Agree.* Opt-out choices that are hidden on a second layer and pre-selected data items, which are not mandatory, are not only violating the affirmative action requirement but also fail to comply with the Data Protection by Default principles (i.e. R12 and R15 are violated). Moreover, information about the data processing purposes is not displayed in the UIs. In other words, required policy information is neither made transparent nor easily accessible as required by R14.

3 PROPOSED SOLUTION

Based on the findings in the previous two sections, we discuss if the identified issues can be addressed by improving transparency, and showing corresponding information in new user interfaces. However, to avoid overwhelming users with a surfeit of information we split the required information into i) the group that is independent from the concrete SP and is required to make an informed choice for the sign-up method (such as pros and cons of the social login option), and ii) the group which is dependent on the particular SP and is required for providing informed consent (such as requested data items, identity of the controller and the purposes of processing). In this section, we discuss how the requirements are addressed by the design of tutorial and new UIs for Facebook social login.

Tutorial. We developed a tutorial aimed at empowering users with informed decisions about their selected method to sign up for an SP in an iterative manner, i.e. integrating feedback from academic experts to improve the content and its understandability. The tutorial can be used independently from concrete user interfaces and it contains two parts: 1) brief process description of sign-up and sign-in, and 2) explanations of the advantages and disadvantages. The first part, describing the steps involved in each method, mainly addresses the following two requirements: *R1* and *R4.* The second part explains the advantages and disadvantages of the social login compared to manual sign-up methods. The elaboration on disadvantages of the social login method in the tutorial also includes some information about the phishing problem, and the conditions of data sharing in the context of social login, e.g. write access and validity duration of access, which may cause privacy issues. Consequently, the second part addresses requirements *R1*, *R3*, and *R6* identified in Section 3.2, and in particular the possibility of the write access and duration of access granted.

Moreover, advantages and disadvantages of social logins in comparison to the manual sign-up method listed in the tutorial were identified from the literature such as [2, 4, 11, 20, 24] and brainstorming with academic experts. The advantages and disadvantages encompass user related issues and are classified into two categories: (1) authentication-related items and (2) items related to data sharing. The authentication-related advantage is that no new password is required for every registration for a website and the disadvantage in this category is the fact that the social network is the single point of failure. Relevant to data sharing, using social logins saves users' time, most importantly, when they want to sign up for a website. On the other hand, the disadvantage is mostly about lack of privacy. Evaluating the effects of the tutorial in Section 5.1, we considered these four advantages and disadvantages. The detailed descriptions of the evaluations are made available separately online with the content of the tutorial[4].

Note, for both sign-up methods we consider that the same information is requested from the SP and, as it is varying based on the specific SP, the relevant knowledge (i.e. requested information from users in each method) is omitted from the tutorial and is provided on the sign-up page of the SP (*R2*).

User Interfaces and Informed Consent. Aiming to address the related requirements in Section 2 to help users give informed consent, we developed new interfaces for the sign-up process using Facebook SSO. Here, we describe how the end user and legal requirements given in Section 2) are met by the proposed interfaces. The proposed user interfaces are depicted in Figures 2 and 3.

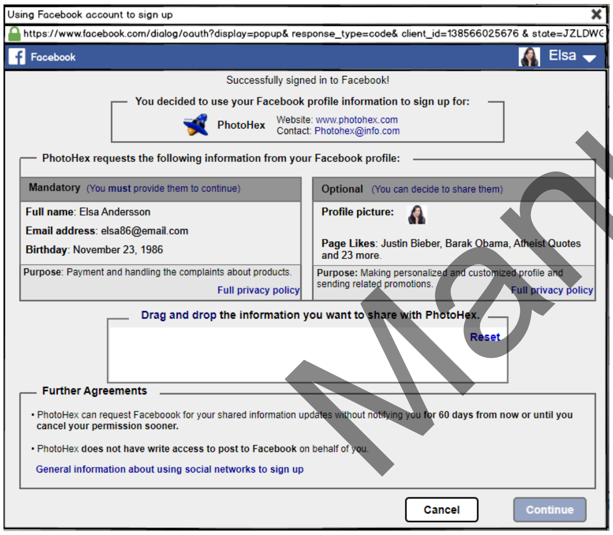
To actively involve users with an affirmative action in the selection of their personal information to share (*R12*), instead of preselected checkboxes, the method of Drag and Drop has been exerted. Pettersson et al. suggest using the Drag And Drop Agreements (DADAs) [18] as an alternative way for users to express consent by moving graphic representations of their data to receivers' locations on a map. The user did not only have to pick a set of predefined data but had to choose the correct personal data symbol(s) and drop them on the correct receiver symbol. However, it remained as a proposal and was never tested in usability studies. Section 7 elaborates more on alternative designs for obtaining informed consent. In our newly proposed UIs, we have one receiver who is the SP, rather than having several. Users should drag the mandatory information, or optional information, and drop it to a unique specific box (Figure 2) to indicate what they want to share. They further click the corresponding button to accept sharing of what they selected. However, when innovative interfaces become prevailing, habituation might re-appear and detract from the reported short-term benefits [5]. Thus, to make the proposed UIs robust against habituation and to meet *R7* requirement, each data item could have a specific place in the white box represented by a meaningful relevant icon, for example. However, testing it against habituation is deferred for future work. It should be noted that data items to be shared are considered separately and not as a set of Public Profile (*R9*) as in current Facebook SSO interfaces (Figure 1).

Our proposed authorisation dialogues contain multi-layered privacy notices to meet requirement R14. The information required in *R6*, *R10* and the legal requirement *R13* are provided as part of the top-layer short privacy notice. In the UI, optional data is clearly marked and separated from the mandatory data (R15). We first provide the identity of the SP and the purposes of data sharing to meet *R13* and *R14*. Furthermore, information about duration of access, the level of access the SP gets (e.g. write or read access), the possibility of access revocation, not sharing the IdP credentials with the SP and independence of sharing personal information from

[4] https://slandtutorial.wordpress.com/

privacy settings on the IdP (Figure 2) are also provided to meet *R5-6*, *R8*, *R10*, *R13* requirements. Besides, clearly visible links to the full privacy policy are provided (R14).

However, it is a well-known problem that users often ignore privacy notices, as they are long, time-consuming to read and difficult to understand. Furthermore, providing too many or repetitive privacy notices can result in habituation: users repeatedly click on notices without considering their content. Even with short, multi-layered privacy notices, much of the information may not seem relevant to users. Many data practices are anticipated and obvious, may not cause concern, or may not apply to a user's current interaction with an SP [19]. Another approach is to force interaction with a notice which can reduce habituation effects [6]. Rowbotham et al. demonstrated that combining an introductory video, standard consent language, and an interactive quiz on a tablet-based system can improve comprehension of clinical research study procedures and risks [22]. Therefore, we designed a second authorisation dialogue (Figure 3) to actively involve users and force them to pay attention to the conditions of data sharing, by integrating the question and answer method (Q&A). Users must answer some questions and check their responses. In the case of wrong answers, the correct responses are shown to the users who must select the right answers and check them again. When answering the questions, users can revert to the first authorisation dialogue and read the short notices.


Using Facebook account to sign up

https://www.facebook.com/dialog/oauth?display=popup& response_type=code& client_id=138566025676 & state=JZLDWG

Successfully signed in to Facebook!

You decided to use your Facebook profile information to sign up for:

PhotoHex Website: www.photohex.com Contact: Photohex@info.com

PhotoHex requests the following information from your Facebook profile:

Mandatory (You **must** provide them to continue)

Full name: Elsa Andersson

Email address: elsa86@email.com

Birthday: November 23, 1986

Purpose: Payment and handling the complaints about products.

Full privacy policy

Optional (You can decide to share them)

Profile picture:

Page Likes: Justin Bieber, Barak Obama, Atheist Quotes and 23 more.

Purpose: Making personalized and customized profile and sending related promotions.

Full privacy policy

Drag and drop the information you want to share with PhotoHex.

Reset

Further Agreements

- PhotoHex can request Faceboook for your shared information updates without notifying you **for 60 days from now or until you cancel your permission sooner.**
- PhotoHex **does not have write access to post to Facebook** on behalf of you.

General information about using social networks to sign up

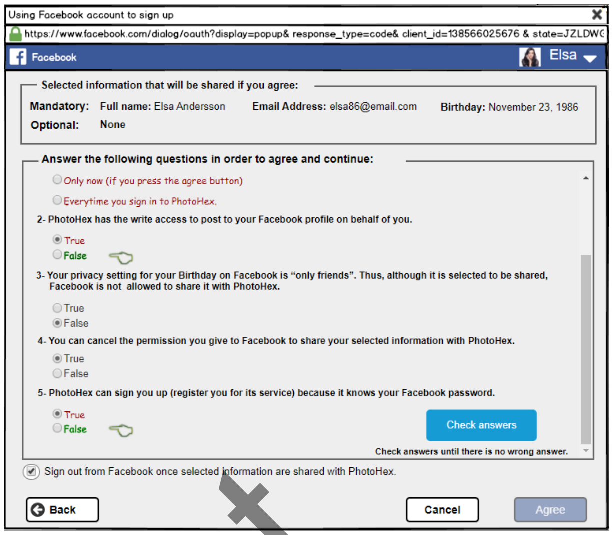
Figure 2: Drag&Drop interface (first authorisation dialogue)

4 METHODOLOGY AND STUDY DESIGN

The purpose of our user study is twofold: 1) to evaluate if reading the tutorial helps users to make better-informed decisions, i.e. informed choices when they select a method to sign up for a website, and 2) to analyse the extent that the new interfaces helps users make better-informed consent when granting permission to share their personal data, in comparison to the Facebook social login UIs.

Framing these questions as hypotheses, we tested the following:

H1: Compared to the user group who do not read the tutorial, users who receive the tutorial make better-informed decisions when they select a sign-up method. In other words, they have a better understanding of the advantages and disadvantages of the sign-up methods they select, than users who do not receive the tutorial.


Using Facebook account to sign up

https://www.facebook.com/dialog/oauth?display=popup& response_type=code& client_id=138566025676 & state=JZLDWG

Selected information that will be shared if you agree:

Mandatory: **Full name:** Elsa Andersson **Email Address:** elsa86@email.com **Birthday:** November 23, 1986

Optional: None

Answer the following questions in order to agree and continue:

○ Only now (if you press the agree button)

○ Everytime you sign in to PhotoHex.

2- PhotoHex has the write access to post to your Facebook profile on behalf of you.

● True

○ False

3- Your privacy setting for your Birthday on Facebook is "only friends". Thus, although it is selected to be shared, Facebook is not allowed to share it with PhotoHex.

○ True

● False

4- You can cancel the permission you give to Facebook to share your selected information with PhotoHex.

● True

○ False

5- PhotoHex can sign you up (register you for its service) because it knows your Facebook password.

● True

○ False

Check answers

Check answers until there is no wrong answer.

☑ Sign out from Facebook once selected information are shared with PhotoHex.

Figure 3: Q&A interface (second authorisation dialogue)

H2a: Users who use the new interfaces have a better understanding of how, and under which conditions, permission is granted, compared to the group who experience the current Facebook SSO interfaces. Specifically, the users of the new interfaces know better about the irrelevance of Facebook privacy settings, and corresponding shared data items (*R8*), the possibility of access revocation (*R10* and *R13*) and the fact that the SPs do not know about their credentials of the IdP (*R5*).

H2b: Users who use the new interfaces have a better understanding of the data items to which access is granted (and to which access is not granted) during the authorisation process compared to the group who experience the current Facebook SSO interfaces. Specifically, they know better for which data items and for how long read access is granted (or not granted) and if the write access is granted to the SP (*R6*, partly *R13*).

4.1 Ethics, Recruitment & Demographics

All necessary steps were taken to adhere to the Swedish Research Council's principles of ethical research [28]. This includes obtaining informed consent, not using participants' actual or sensitive data to sign up and debriefing participants at the end of the study.

Participants were recruited via social media, mailing lists, paper flyers posted across the university and at public places in the city center. When signing up for an appointment in the lab, participants were asked to confirm their eligibility that they were at least 18 years old and had a Facebook account. Participants were randomly assigned to one of four groups of the study. They received either a lunch coupon for the university canteen or a present card on completion of the study, depending on where they were recruited.

In total 80 people, all of whom had Facebook accounts, participated in our study. Among them, 45 had already experienced Facebook login. The age range is 19 - 60 years (M=32.7, SD=10.7).

Except for four who have high school degree level only, the other participants have, or are pursuing, various third level educational subjects, including Psychology, Political Science, Applied Mathematics, Geography, Nursing, Architecture. One has a degree in Computer Engineering. Table 1 shows our participants' demographics. Using the IUIPC questionnaire (ten questions - IUIPC for control, awareness and collection, with a 7-point Likert scale)[5] we assessed that participants are rather concerned (M=56.31, SD=8.65, Min=27, Max=70) about information privacy.

Table 1: Demographics – in total and per group

Properties	Total (n=80)	G4 (n=20)	G3 (n=20)	G2 (n=20)	G1 (n=20)
Age					
18-25	25	6	6	5	8
26-32	23	7	5	5	6
33-39	14	2	4	4	4
40-46	7	3	0	3	1
47-53	5	1	3	1	0
54-60	6	1	2	2	1
Gender					
Male	31	8	7	7	9
Female	49	12	13	13	11
Educational background					
High school	4	1	1	1	1
Bachelor	37	9	11	8	9
Master	19	8	2	4	5
PhD	20	2	6	7	5
English proficiency level					
Elementary	6	1	2	2	1
Limited	16	5	4	3	4
Professional	25	6	6	5	8
Full profess.	25	8	5	7	5
Native	8	0	3	3	2
Privacy concern values using IUIPC for awareness, control and collection					
Mean	56.31	55.50	53.00	58.55	57.75
SD	0.97	2.02	2.10	1.55	1.92
Using password manager					
No	59	18	12	16	13
Yes	19	2	7	4	6
Do not know	2	0	1	0	1
Previous experience of Facebook SSO login					
No	31	6	7	9	9
Yes	45	11	12	11	11
Do not know	4	3	1	0	0

4.2 Study Design

A functional mock-up of the sign-up process for a ficticious photo printing website, PhotoHex, was developed using Axure prototyping tool. The mock-up provided the entire interfaces needed to sign up to the website using Facebook SSO, both simulating the real Facebook interfaces and our proposed UIs (Figures 2 and 3).

A between-subject study with four groups was conducted: Group 1 (G1) read the tutorial and signed up using the new interfaces, Group 2 (G2) did not receive the tutorial and signed up using the new interfaces, Group 3 (G3) read the tutorial and signed-up using current Facebook interfaces, and Group 4 (G4) did not receive the tutorial and signed up using current Facebook interfaces.

We conducted the study with participants individually. Since we did not want our participants to be primed for privacy we did not reveal our full study purpose, until afterwards. We carefully and ethically obfuscated the purpose, both during the recruitment phase and during our interactions with participants in the study session, using some dummy questions. The stated goal of the study was introduced as a usability test of a photo printing website, PhotoHex, and we advised the true goal of the study in the debriefing session.

Figure 4 provides an overview of the study design and the collected data types. The study is divided into the following phases:

Welcome and Demographics: The moderator welcomed and thanked the participants, provided them with information about the study and the PhotoHex website and asked them to sign the informed consent form for participation. After signing, they were requested to complete the survey, starting with demographics (including familiarity with English[6]). Participants' privacy concerns were then assessed using the IUIPC. At the end of this first phase, participants were informed that PhotoHex website provides either a manual sign-up for an account, or a Facebook social login.

Tutorial: Next, those assigned to complete the tutorial, G1 and G3, were prompted to contact the study moderator to receive the tutorial, provided on paper. Once finished reading the tutorial, they were asked to complete the survey. Those participants in G2 and G4 simply completed the survey, without intervention.

Sign-up Option: Participants were asked the sign-up option they preferred to use for the PhotoHex website. They were invited to justify their decisions, and to provide the advantages and disadvantages of the method they selected, in free-text.

Role Play: Independent of the method chosen in the Sign-up phase, participants received some instructions about signing up for the PhotoHex website using the Facebook SSO option, while role-playing a persona called Elsa. Information on Elsa was provided on a role-playing card that included her Facebook credentials. Using a persona serves a dual purpose: 1) it allows full control of the information each participant encounters, providing a standard experience that can be compared between participants, and 2) ethical reasons: it helps us avoid handling sensitive participant information, which needs to be disclosed for the study, e.g. birth dates or page likes on Facebook. Although role-playing may affect the ecological validity of results it is not severely affecting comparisons between different tests as the premises remain the same.

Task on the website: Participants signed-up using either the new interfaces or the old ones.

Questions about the experienced task: Once signed-up, the moderator asked participants to continue the survey, answering questions about their experience using PhotoHex. Questions included open and multiple-choice regarding the granted access, as well as questions to deduce the users' satisfaction, using the System Usability Scale (SUS) questionnaire [7]. At the end of this phase, we also asked our participants if they had used Facebook SSO login before our study.

End: At the end, participants were debriefed on the actual purpose of the study, and asked for feedback on the tutorial and interfaces. The instructor then reimbursed and thanked the participants.

5 EVALUATION

This section deals with the effect receiving the tutorial has on the users' ability to make an informed decision when choosing a sign-up method.

[5] Internet Users' Information Privacy Concerns (IUIPC) is developed to measure people's general concerns about organisations' information handling practices [16].

[6] The study was conducted in Sweden, through English.

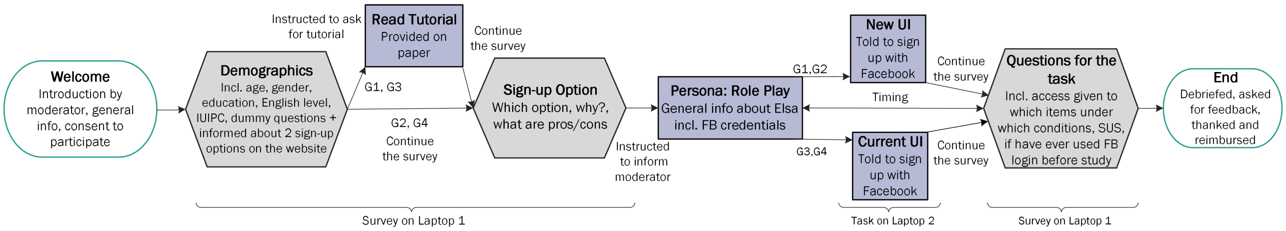

Welcome
Introduction by moderator, general info, consent to participate
Demographics
Incl. age, gender, education, English level, IUIPC, dummy questions + informed about 2 sign-up options on the website
Instructed to ask for tutorial
G1, G3
Read Tutorial
Provided on paper
Continue the survey
G2, G4
Continue the survey
Sign-up Option
Which option, why?, what are pros/cons
Instructed to inform moderator
Persona: Role Play
General info about Elsa incl. FB credentials
G1,G2
G3,G4
Timing
New UI
Told to sign up with Facebook
Current UI
Told to sign up with Facebook
Continue the survey
Continue the survey
Questions for the task
Incl. access given to which items under which conditions, SUS, if have ever used FB login before study
End
Debriefed, asked for feedback, thanked and reimbursed
Survey on Laptop 1
Task on Laptop 2
Survey on Laptop 1

Figure 4: Study design including the paths for the four different groups.

5.1 Tutorial

As described in Section 4.2, saving users' time and not having a need for a new password are the advantages; and being the single point-of-failure and not respecting users' privacy are the disadvantages of the SSO solutions. Considering these, we used a close coding approach for the free-text question. To examine H1 hypothesis, we grouped those who read the tutorial, and groups who did not (G1 + G3 with G2 + G4) and we compared the number of both correct and false advantages and disadvantages mentioned in the free-text questions, based on the selected sign-up method, for each group. UIs could not have any effects on H1 because participants read the tutorial and answered the questions related to it before experiencing the UIs.

Free-text. A Kruskal-Wallis-Test[7] showed significant differences in the correctly identified advantages between participants who received the tutorial and those who did not ($\chi^2(1)$=8.36, p=.004). Participants who received the tutorial were able to identify more advantages correctly (M=1.23, SD=0.58) than participants who did not receive the tutorial (M=0.90, SD=0.38). Although participants who received the tutorial were able to identify more disadvantages correctly (M=0.93, SD=0.57) than participants who did not (M=0.73, SD=0.51), this result is not statistically significant. Figure 5 depicts how often the four items were provided by the participants in the different groups. Participants who did not receive the tutorial were less aware of the fact that using Facebook means there is a single point-of-failure and that this option may cause privacy concerns.

Twelve in the group who received the tutorial, and eight in the group without the tutorial, selected the Facebook SSO and did not mention any false disadvantages or advantages (Figure 5). On the other hand, the fact that sign-up takes less time was erroneously mentioned as an advantage of the manual option among participants who selected this method. Not being privacy friendly compared to the Facebook SSO, and being the single point-of-failure were the false disadvantages listed by participants who selected the manual option.

5.2 UI

This section describes and discusses the effect of the new UIs on users' ability to give informed consent. The results are reported considering two groups who experienced the new UIs and who used the current Facebook interfaces, regardless of reading the tutorial. Since half of the participants who experienced new UIs and half of the participants who used current Facebook SSO dialogues received the tutorial, to test the H2a and H2b hypotheses we checked if receiving the tutorial had an effect on making informed consent, when confronting the authorisation dialogues. We found no significant effect of receiving the tutorial on giving informed consent, including understanding of how, under which conditions, and to which items, access is granted (with all p>.05).

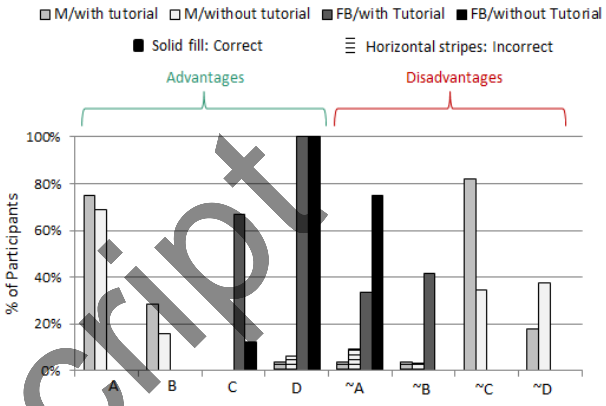


Figure 5: Percentages of participants mentioned each of the items in free-text question (M-manual, FB-Facebook). A: Privacy-friendly, B: No single point-of-failure, C: No need for a new password, D: Sign-up takes less time.

To examine H2a, participants' answers to three statements about Facebook information sharing with PhotoHex described in Table 2 are analysed. In detail, the statements involve participants' comprehensions about the relation between privacy settings in the Facebook profile and sharing information with the SP (S1), access revocation (S2) and sending Facebook credentials to the SP (S3). Using a Kruskal-Wallis-Test[7], we found significant effects for the type of interfaces used on participants' ability to correctly evaluate all three statements (see Table 2), with more participants who used the new interfaces evaluating all three statements correctly than participants who used current Facebook authorisation dialogues as depicted in Figure 6. Thus, H2a is supported.

After completing the sign-up process, participants were presented a list of fifteen different types of personal information as depicted in Figure 7 and had to indicate whether they shared the particular information with PhotoHex or not. In Figure 7, the first three types from the left are mandatory and the next two are optional requested information while the remaining ten are dummy information not requested in the authorisation dialogues. We populated

[7] We used non-parametric tests since the assumptions of normality and homogeneity of variances were violated.

Table 2: Results of the Kruskal-Wallis-Test for participants' ability to correctly evaluate the statements. TF: True/False question. MC: Multiple-Choice question.

Statement	df	χ^2	Sig.
(S1) Your privacy setting for your Birthday on Facebook is only friends. Thus, although it is selected, Facebook is not allowed to share it with the website (TF).	1	12.77	<.001***
(S2) You can cancel the permission you give to Facebook to share your selected information with PhotoHex (TF).	1	10.32	.001**
(S3) The website can sign you up because it knows your Facebook password (TF).	1	8.25	.004**
(S4) PhotoHex has write access to post something to your Facebook profile on behalf of you (TF).	1	21.07	<.001***
(S5) PhotoHex will be able to request the information you selected ...(MC)	1	55.47	<.001***

the list with dummy information to avoid the right answer being the selection of *shared* option for all the requested information. To test H2b, we compared how many of the fifteen presented information types were recalled correctly as *shared* and *not shared*, by the participants who used the new interfaces and those who used the current Facebook authorisation dialogues. Using a Kruskal-Wallis-Test, we found significant differences for the type of interfaces used (χ^2(1)=26.53, p<.001), with participants using the new interfaces recalling a greater number of *shared* and *not shared* information correctly (M=83.50%, SD=24.20%) than participants who used the current Facebook authorisation dialogues (M=48.67%, SD=27.97%).

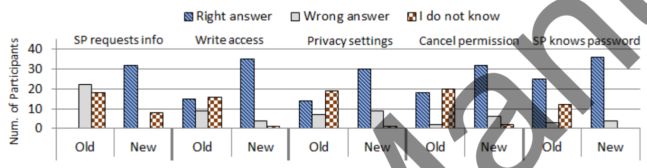


Figure 6: Answers to the statements for the two groups (new or old UIs).

We also measured the number of *not sure* answers for each participant for all listed data types. The Kruskal-Wallis-Test, demonstrated significant differences for the type of interfaces used (χ^2(1)=14.11, p<.001). Participants using the current Facebook authorisation dialogues expressed higher levels of uncertainty (M=5.48, SD=5.12) than participants using the new interfaces (M=1.55, SD=2.86).

Accordingly, we deduce that involving participants more actively in the process of selecting the information to be shared helps them to pay more attention to what was shared, and decreased the level of uncertainty. We further evaluated the effect of using the new UIs on participants' understanding of the access granting process by comparing their answers to two statements addressing their conception about write access (S4) and the duration of the access token (S5). Contrary to other statements which were true/false questions, S5 was a multiple-choice question with five answers among them one was the correct one: PhotoHex can request the information you selected for 60 days or until you cancel your permission. We identified significant effects for the type of interfaces used on participants' ability to correctly evaluate both statements (see Table 2), again with more participants who used the new interfaces evaluating both statements correctly than participants who used current authorisation dialogues of Facebook (see Figure 6). Thus, H2b is also supported.

6 FURTHER FINDINGS AND DISCUSSION

In this section, we report the level of users' satisfaction and efficiency to show the trade-off the new UIs bring and highlight the parts of the proposed UIs requiring potential improvements. We also report the results of the effects of participants' privacy concerns and previous experience of Facebook login on our dependent variables for testing hypotheses (see Section 5.2 and 5.1).

The SUS and efficiency values are displayed in Table 3. The Mean SUS value for the new UIs in total is 61.76 which is although acceptable according to Brooke's work [7], is still low. Using a univariate analysis of variance (ANOVA)[8], we found a significant effect for receiving the tutorial on the SUS values (F(1, 76)=5.62, p=.020, partial η^2=0.07).

The time reported in Table 3 is the duration of sign-up for the website using Facebook SSO in both UIs. Using a Kruskal-Wallis-Test, no effect of receiving the tutorial was found on the efficiency (χ^2(1)=0.62, p=.43). The total time to complete the sign-up process using the new UIs is approximately 3 and 4 times more than the time required for signing up using the current Facebook UIs for the group who read the tutorial and who did not, respectively. However, the efficiency of the Facebook UIs is achieved by not adhering to legal requirements of the GDPR that may be time-consuming for users. A simple click-through dialogue providing insufficient policy information is presented with opt-out (instead of opt-in) choices hidden on a second layer that only appears if the user clicks on the *Edit This* link. This means that the user can simply click *Continue as [user's name]* (Figure 1) without being confronted with required policy information (such as, on the data processing purposes) that should be read, and without having to do any active affirmative actions or choices for selecting the data items to be shared (i.e. as pointed out in Section 2.2, R12, R13, R15 are violated). If Facebook implemented effective UIs that were legally compliant with the GDPR, they would also demand more activities from the user and could therefore not be as efficient as the current Facebook interfaces.

For the new UIs, the reported time consists of the time to authenticate to Facebook (entering the username and password), time for sharing information using DADA and time to answer the quiz questions (Q&A). The Mean time for DADA is 78.70s for the group who read the tutorial and 94.50s for the rest. The Mean time for Q&A is 115.75s and 135.65s respectively. The time for DADA and Q&A time is dependent on the number of information to be shared and the questions to be answered, accordingly. Less mandatory information requested to be shared, and eliminating statements not dependent on the specific service provider in Q&A, and including them in Q&A just for the first time a user selects the Facebook as an IdP on a website, contribute to the reduction in time.

Regarding the tutorial, a Kruskal-Wallis-Test showed no significant relationship between the previous experience of Facebook

[8] The assumptions of normality and homogeneity of variance were satisfied.

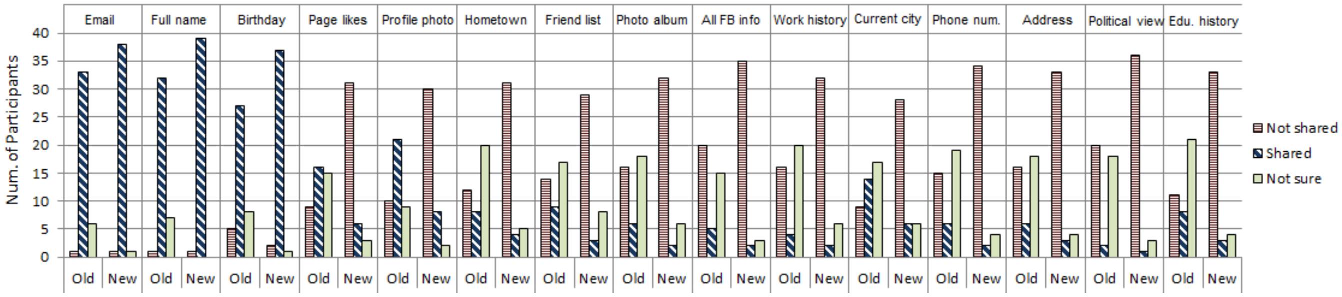


Figure 7: Number of information recalled as shared, not shared or not sure by participants who used the new and the old UIs.

login and the number of correctly and falsely identified advantages and disadvantages. IUIPC values, and IUIPC awareness values, are also not significantly correlated with advantages and disadvantages mentioned by participants. Finally, considering UIs, previous experience of Facebook login and IUIPC values, and IUIPC awareness values, are not significantly correlated with number of correctly recalled personal information as *shared* or *not shared*, and the ability to correctly evaluate the five statements, except for statement S5 and S2. Using non-parametric Spearman's rank correlation, there is a significant positive relationship between the ability to correctly evaluate S5 and the IUIPC awareness values for participants who said they would choose the manual option to sign up for PhotoHex website (ρ = .257, p=.047*) and a significant positive relationship between the ability to correctly evaluate S2 and the IUIPC awareness values for participants who said they would choose the Facebook login (ρ = .566, p=.009**).

Table 3: Perceived usability (SUS values) and the efficiency (time) of current UIs (C) and new UIs (N) participants experienced.

Without tutorial				With tutorial	
Type of UI		SUS	Time(s)	SUS	Time(s)
C (n = 40)	M	73.25	70.85	75.88	74.15
	SD	13.55	39.62	12.49	37.26
N (n = 40)	M	56.13	291.40	67.38	240.65
	SD	11.96	83.79	14.22	78.43

7 RELATED WORK

The related work of this paper includes research relevant to proposing informational tutorials and research related to improving informed consent.

Prior work on the effectiveness of tutorials has mostly tried to change users' attitudes toward online behaviour and security tools, and techniques. For example, Albayram et al. [1] investigated the effectiveness of informational videos on improvements in users' adoption rate of two-factor authentication. However, Albayram et al. [1] did not directly measure the gain in participants' post video knowledge. Contrary, with the proposed tutorial in this paper we did not want to nudge users' behaviours towards a specific method for sign-up. However, the aim was to improve users' knowledge about the available options which could help them to make decisions consciously. In the context of social logins, Ronen et al. [21] also observed changes in users' selection of sign-up methods, with different identity providers, after they were exposed to the benefits they would receive, and the personal information they had to share, for each individual option.

Earlier work on helping users to be aware of the information they share and preventing leakage of personal information in the context of social login has proposed different methods. In particular, a proposal from Wang et al. [29] suggests new interfaces based on the limitations of Facebook authorisation dialogues at the time of preparing their work. However, the extent to which the users might understand and pay attention to what was actually shared using the proposed new interfaces was not evaluated. Javed and Shehab [12] investigated the effects of animated authorisation dialogues for Facebook. Another proposal by Javed and Shebab [13] used eye tracking in order to force users to read the permission dialogue but they did not report about the cost to users in terms of time and satisfaction. Also, Karegar et al. [14] studied users' recall of personal information disclosure in authorisation dialogues in which desired data could be selected by checking boxes. They also investigated the effect of previewing the selected information on improving users' attention before giving consent.

An early work in HCI solutions for informed consent was done by the PISA project as a pioneer, as pointed out in Section 2, which conducted important research on how to map legal privacy principles to possible HCI design solutions [17], suggesting the concept of *Just-In-Time-Click-Through Agreements* (JITCTAs) as a possible solution for obtaining consent. Two-clicks (i.e. one click to confirm that one is aware of the proposed processing, and another one to consent to it) or ticking a box have also been suggested by different European legal experts and data commissioners as a means for representing the data subject's consent [18]. Pettersson et al. [18], building on PISA project results, developed the alternative concept of DADAs, to address the problem of habituation, to which JITCTAs are vulnerable. In this paper, we adapted the DADAs to fit our context for selecting the personal information to be shared with the SP using Facebook SSO.

To the best of our knowledge, there is no prior work trying to enforce informed consent while measuring it, considering the legal requirements in a user study. In our proposed interfaces aligned with GDPR, personal information is not selected by default and users are actively involved in selection. Moreover, conditions of data sharing have received special attention; being aware of such information is necessary for a consent to be considered informed, and informed consent is measured as a function of users' knowledge about what they share under which conditions.

8 CONCLUSION

Our objective in this work is to empower users to make informed decisions in the context of signing up for an SP using a social network as an IdP. A tutorial was designed to inform users on the pros and cons of using social logins. Moreover, we designed UIs for enabling informed consent for sharing personal information, following the approaches of human-centered and privacy by design by addressing end user-specific and legal privacy requirements from the beginning and throughout the UI development cycle. Our evaluations show that the tutorial notably helps users to improve their knowledge about the benefits of options they have for sign-up, however, more investigations are required to ideally communicate the pros and cons of services that may threaten the users' privacy. For our proposed UIs, informed consent was enforced with the help of an active involvement of users via 'Drag and Drop' and 'Question and Answer'. A between-subject user study shows that our new UIs are significantly more effective in helping users to provide informed consent comparing to the current authorisation dialogues of the social network. Hence, affirmative actions like 'Drag and Drop' that require users to carefully check opt-in choices, as well as interactive knowledge testing and feedback, are examples of effective HCI concepts for informed consent UIs. However, their use comes at a cost. We continue to work on decreasing the gap between legally compliant authorisation dialogues and usable user-centric ones, while considering different modes of affirmative actions which could potentially direct users' attention to information they disclose, the robustness of methods against habituation, and the effects of providing data processing purposes.

ACKNOWLEDGEMENT

This research has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 653454. It is also supported by the German Federal Ministry of Education and Research (BMBF) within MoPPa and co-funded by the DFG as part of project D.1 within the RTG 2050 "Privacy and Trust for Mobile Users". The authors thank Bridget Kane for proofreading the manuscript and John Sören Pettersson, Henrik Andersson, and Maria Wahl for their help in reaching more participants.

REFERENCES

[1] Yusuf Albayram, Mohammad Maifi Hasan Khan, and Michael Fagan. 2017. A Study on Designing Video Tutorials for Promoting Security Features: A Case Study in the Context of Two-Factor Authentication (2FA). *International Journal of HumanâĂŞComputer Interaction* 33, 11 (2017), 927–942.

[2] Majid Arianezhad, L Jean Camp, Timothy Kelley, and Douglas Stebila. 2013. Comparative Eye Tracking of Experts and Novices in Web Single Sign-on. In *CODASPY*. ACM, 105–116.

[3] Art. 29 Data Protection Working Party. 2004. Opinion 10/2004 on More Harmonised Information Provisions. Available from: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf. (2004).

[4] Lujo Bauer, Cristian Bravo-Lillo, Elli Fragkaki, and William Melicher. 2013. A Comparison of Users' Perceptions of and Willingness to Use Google, Facebook, and Google+ Single-sign-on Functionality. In *DIM*. ACM, 25–36.

[5] R. Böhme and S. Köpsell. 2010. Trained to Accept?: A Field Experiment on Consent Dialogs. In *CHI*. ACM, 2403–2406.

[6] Cristian Bravo-Lillo, Lorrie Cranor, Saranga Komanduri, Stuart Schechter, and Manya Sleeper. 2014. Harder to Ignore? Revisiting Pop-Up Fatigue and Approaches to Prevent It. In *SOUPS*. USENIX Association, 105–111.

[7] John Brooke. 2013. SUS: A Retrospective. *Journal of Usability Studies* 8, 2 (2013), 29–40.

[8] Ann Cavoukian. 2009. Privacy by Design: The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices. *Information and Privacy Commissioner of Ontario, Canada* (2009).

[9] Serge Egelman. 2013. My Profile is My Password, Verify Me!: The Privacy/Convenience Tradeoff of Facebook Connect. In *CHI*. ACM, 2369–2378.

[10] Batya Friedman, Edward Felten, and Lynette I. Millett. 2000. Informed Consent Online: A Conceptual Model and Design Principles. *University of Washington Computer Science & Engineering Technical Report 00–12–2* (2000).

[11] Ruti Gafni and Dudu Nissim. 2014. To Social Login or not Login? Exploring Factors Affecting the Decision. *Issues in Informing Science and Information Technology* 11 (2014), 57–72.

[12] Yousra Javed and Mohamed Shehab. 2016. Investigating the Animation of Application Permission Dialogs: A Case Study of Facebook. In *DPM*. Springer, 146–162.

[13] Yousra Javed and Mohamed Shehab. 2017. Look Before You Authorize: Using Eye-Tracking to Enforce User Attention Towards Application Permissions. *PoPET* 2, 2 (2017), 23–37.

[14] Farzaneh Karegar, Daniel Lindegren, John Sören Pettersson, and Simone Fischer-Hübner. 2017. Assessments of a Cloud-Based Data Wallet for Personal Identity Management. In *Information Systems Development: Advances in Methods, Tools and Management (ISD2017 Proceedings)*.

[15] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. 2010. *Research Methods in Human-Computer Interaction*. Wiley Publishing.

[16] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15, 4 (2004), 336–355.

[17] Andrew S. Patrick and Steve Kenny. 2003. From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interactions. In *PET*. Springer, 107–124.

[18] John Sören Pettersson, Simone Fischer-Hübner, Ninni Danielsson, Jenny Nilsson, Mike Bergmann, Sebastian Clauss, Thomas Kriegelstein, and Henry Krasemann. 2005. Making PRIME Usable. In *SOUPS*. ACM, 53–64.

[19] Ashwini Rao, Florian Schaub, Norman Sadeh, Alessandro Acquisti, and Ruogu Kang. 2016. Expecting the Unexpected: Understanding Mismatched Privacy Expectations Online. In *SOUPS*. USENIX Association, 77–96.

[20] Nicky Robinson and Joseph Bonneau. 2014. Cognitive Disconnect: Understanding Facebook Connect Login Permissions. In *COSN*. 247–258.

[21] Shahar Ronen, Oriana Riva, Maritza Johnson, and Donald Thompson. 2013. Taking Data Exposure into Account: How Does It Affect the Choice of Sign-in Accounts?. In *CHI*. ACM, 3423–3426.

[22] Michael C Rowbotham, John Astin, Kaitlin Greene, and Steven R Cummings. 2013. Interactive Informed Consent: Randomized Comparison with Paper Consents. *PloS one* 8, 3 (2013), e58603.

[23] San-Tsai Sun, Eric Pospisil, Ildar Muslukhov, Nuray Dindar, Kirstie Hawkey, and Konstantin Beznosov. 2011. What Makes Users Refuse Web Single Sign-on?: An Empirical Investigation of OpenID. In *SOUPS*. ACM, Article 4, 20 pages.

[24] San-Tsai Sun, Eric Pospisil, Ildar Muslukhov, Nuray Dindar, Kirstie Hawkey, and Konstantin Beznosov. 2013. Investigating Users's Perspectives of Web Single Sign-On: Conceptual Gaps and Acceptance Model. *TOIT* 13, 1, Article 2 (2013), 35 pages.

[25] The European Parliament and the Council of the European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). (2016).

[26] Pagona Tsormpatzoudi, Bettina Berendt, and Fanny Coudert. 2015. Privacy by Design: From Research and Policy to Practice–the Challenge of Multi-disciplinarity. In *APF*. Springer, 199–212.

[27] Anna Vapen, Niklas Carlsson, Anirban Mahanti, and Nahid Shahmehri. 2015. Information Sharing and User Privacy in the Third-party Identity Management Landscape. In *CODASPY*. ACM, 151–153.

[28] Vetenskapsrådet. 2002. *Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning.*

[29] Na Wang, Jens Grossklags, and Heng Xu. 2013. An Online Experiment of Privacy Authorization Dialogues for Social Applications. In *CSCW*. ACM, 261–272.