Behaviour & Information Technology

ISSN: 0144-929X (Print) 1362-3001 (Online) Journal homepage: https://www.tandfonline.com/loi/tbit20

An evaluation of three designs to engage users when providing their consent on smartphones

Daniel Lindegren, Farzaneh Karegar, Bridget Kane & John Sören Pettersson

To cite this article: Daniel Lindegren, Farzaneh Karegar, Bridget Kane & John Sören Pettersson (2019): An evaluation of three designs to engage users when providing their consent on smartphones, Behaviour & Information Technology, DOI: 10.1080/0144929X.2019.1697898

To link to this article: https://doi.org/10.1080/0144929X.2019.1697898

Published online: 17 Dec 2019.

BEHAVIOUR & INFORMATION TECHNOLOGY
https://doi.org/10.1080/0144929X.2019.1697898

An evaluation of three designs to engage users when providing their consent on smartphones

Daniel Lindegren[a], Farzaneh Karegar[b], Bridget Kane[a] and John Sören Pettersson[a]

[a]Information Systems, Karlstad University, Karlstad, Sweden; [b]Computer Science, Karlstad University, Karlstad, Sweden

ABSTRACT

The graphical and interactive design of a consent form helps individuals to keep control and pay attention to the information that they are disclosing. In the context of mobile apps we propose and test alternative interaction design solutions for selecting personal information on permission dialogues, namely using checkboxes, a drag-and-drop selection, and a swiping action. We test each proposed design and compare the results in terms of their usability and effectiveness in helping users to be more attentive and aware of their data flow, in other words, to provide their informed consent. This study demonstrates that checkboxes while speedy do not engage the user as much as drag-and-drop or swiping. User satisfaction is positively impacted by these newer ways of giving consent.

ARTICLE HISTORY
Received 6 February 2019
Accepted 20 November 2019

KEYWORDS
Consent form; usable privacy; user awareness; permission dialogues; user interfaces; personal data

1. Introduction

The collection of digital information by service providers (SPs) is an increasing and important trend over the last decade. Although digital information creates new opportunities for both service providers and users, for example by enabling faster methods for authentication or providing knowledge-based decision-making, digital information raises new challenges regarding an individual's privacy. Nowadays, users are often requested to waive their rights and register a personal account, if they wish to access a service provider, and users are required in the process of registration to disclose (some of) their personal information.

Registration to a service provider can be carried out by directly completing a form, or using an identity provider (IdP) if offered by the service provider. In contrast to the direct registration method for SPs, using an identity provider relieves users of the need to remember many sets of usernames and passwords. On one hand, using an IdP is less time consuming because the personal information is forwarded directly from the IdP to the SP. On the other hand, the identity provider learns to which services, and when, its customers communicate while having access to the plain-text personal data. For example, nowadays we have social networks which also act as IdPs. Such IdPs gradually build detailed user profiles from users' data which is a privacy threat for individuals. To reduce the effects of providing convenience at the expense of privacy in the context of IdPs, some research, such as the CREDENTIAL project (Kostopoulos et al. 2017) on cloud technology for identity access management, has been conducted. That project provided solutions for privacy-preserving identity providers, which do not have access to the data in plain-text. The technology provides its services through a mobile app, the CREDENTIAL Wallet app, which acts as an IdP and a data access manager. Solutions such as the CREDENTIAL project, which benefits from new technologies such as proxy re-encryption (Hörandner et al. 2016), will not be fully effective for individuals in preserving their privacy without considering their understanding and awareness of data flow between service providers and identity providers.

Privacy concerns, in the context of IdPs, may stem from the design problems in consent forms which do not help users to give their consent while, at the same time, keep the individual fully informed. Designing interfaces for users to give their consent is challenging. It should be possible to inform users, simply, about how their data will be used, and the purpose for which it is required. It should also be possible for users to give permission to use specific items of information in a particular context only, i.e. with restricted consent. There are scenarios in healthcare for example, where it is critically important that a patient undergoing a

CONTACT Bridget Kane bridget.kane@kau.se

procedure understands the risks and benefits of the procedure, and can provide their informed consent, or not, to proceed. The person is also entitled to know for what purpose their information is needed and how their privacy will be respected. Efforts are on-going to design interfaces with these types of scenarios in mind (Assale, Barbero, and Cabitza 2019); and there is an acceptance that generic systems need to be developed and implemented that will be simple, easy, and quick for users.

Permission dialogues in the context of identity providers, also known as authorisation dialogues, are one type of consent forms that users encounter in their everyday life. Permission dialogues are widely used in today's digitised world on mobile phones and desktop computers to authorise the mobile and desktop applications that access users' personal data and resources on their devices, based on their permission settings. Previous studies (Bauer et al. 2013; Karegar et al. 2018a) show that providing users with permission dialogues without the possibility to choose the information to share, or with opt-out instead of opt-in choices, makes it difficult for users to notice and control their personal data. In addition, some researchers reported that users desire to keep control over their data and manually select the information to be shared rather than having their data selected by default (Karegar et al. 2018b). Being informed of the personal data flow while giving their consent, and users' active actions showing their clear intention to agree to data processing, will help users to better preserve their privacy and control their data; and it is decreed by law. If the legal basis of data processing is consent, services should obtain informed consent from users that must be specific, unambiguous, and freely given by an affirmative action, which is an indication of users' understanding and willingness to agree to the processing of their personal data, according to Art. 4 (11) of the EU General Data Protection Regulation (GDPR) (The European Parliament and the Council of the European Union 2016).

However, the GDPR, while specifying the legal requirements of the consent and the need for affirmative actions, which can include ticking a box or changing technical settings, does not clarify to what degree affirmative actions such as ticking boxes are effective for obtaining informed consent. In other words, there is a gap between the legal requirements of consent and the design of user interfaces to achieve informed consent. In addition, although in some previous work (Karegar et al. 2018b), researchers utilised ticking boxes for data selection on the consent forms it did not help users to pay attention to details of data disclosures and remember all of the personal data they agreed to share. Karegar et al. (2018a) utilised the Drag And Drop (DAD) to actively involve users in data selection. Although DAD significantly helped users to recall the information they agreed to share compared to the dialogues using opt-out choices, it is not yet clear if the DAD design can help users better than other opt-in choices that actively engage users when requesting their consent. There is, therefore, a need to investigate and compare alternative possible design solutions for the opt-in choices that actively involve users with the content, and measure their effectiveness compared to common practices such as checkboxes.

In this paper, we contribute to decreasing the gap between requirements of informed consent and the design of user interfaces for consent dialogues. We investigate three interactive techniques, namely DAD, checkbox, and swiping, that actively involve users in the process of giving consent via permission dialogues of IdPs on mobile devices. Different interaction techniques entail different actions. As a result, the interaction techniques may differ in how they are perceived by users and the cognitive efforts they require (Sundar et al. 2014). Therefore, the interactive techniques utilised in this paper which facilitate users to actively select personal information are compared in terms of their usability and effectiveness to help users to be more attentive and aware of data flow. We report on three user studies ($n = 3 \times 20$), each conducted to test a specific interactive design option, with sixty participants in total, and show that different interface designs have a notable impact on their perceived usability.

The remainder of this paper is structured as follows: Section 2 presents related research. Section 3 is devoted to methodology and study design. The graphical representations of the three interaction techniques utilised in our user interfaces are described and explained in Section 4. Section 5 presents the results. Analysis and discussion are reported in Section 6. Finally, Section 7 concludes the paper by restating the important findings as well as their implications for future investigations.

2. Related work

Sundar (2007) proposes a theoretical model about the psychological effects of interactivity. This model of interactivity effects has three distinct types of interactivity: (i) source, (ii) message, and (iii) medium of communication. Medium-based interactivity, i.e. different interaction techniques which are the focus of our study, refers to the different ways in which an interface affords its users to interact with information, for example, access information or select among options. According to the model, differences in interaction techniques can affect how users evaluate, engage with, and

process the content of the interface which in turn can affect user cognition and attitudes.

Guided by the theoretical model of interactivity effects (Sundar 2007), Sundar et al. (2014) compared six different types of interaction techniques, namely click-to-download, dragging, hovering, sliding, zooming in and out, and flipping, in the context of informational websites on desktop. Their results support the theoretical assumptions of the model of interactivity effects: some interaction techniques, e.g. sliding, are better than others to positively affect learning outcomes such as content recall.

There are several works that try to catch user attention to different privacy and security notices including consent forms, either by including some eye-catchers in the user interface (e.g. Brustoloni and Villamarín-Salomón 2007; Bravo-Lillo et al. 2013; Javed and Shehab 2016; Tabassum et al. 2018) or by employing interaction techniques to engage users with the content (Bravo-Lillo et al. 2013; Wang, Grossklags, and Xu 2013; Karegar et al. 2018a, 2018b).

For example, employing checkboxes as the interaction technique, Wang, Grossklags, and Xu (2013) suggest new interfaces that consider the limitations of Facebook permission dialogues to help users to make informed consent. In the new interfaces, users have the opportunity to opt out from disclosing their personal information using checkboxes. However, the extent to which the users might understand and pay attention to the information that was actually shared using the proposed new interfaces was not evaluated and Wang, Grossklags, and Xu (2013) work is limited to the exact characteristics of Facebook dialogues at the time of their study. Although Wang, Grossklags and Xu did not measure if their proposed new interfaces actually increased a user's attention to what the user shared, they report that participants who used the new checkbox-enabled interfaces released significantly less information in total and opted out from certain data collection compared to the participants who used control permission dialogues that lack any options.

Bravo-Lillo et al. (2013) investigated the effects of visual attractors for computer security warnings on user attention to the most important information, the salient field, for making decisions. The attractors Bravo-Lillo et al. (2013) used compromised purely visual attractors and inhibitive attractors[1] which included the swiping and type attractors that actively engaged users with the salient field. The swiping attractor required users to move their mouse over the salient field, from left to right, to highlight the letters which is different from the swiping action on mobile devices used in our study (see Section 4 for more details on the swiping action in our study). The type attractor required the user to retype the contents of the salient field. The salient field included either a suspicious or a benign request and the effectiveness of attractors on user attention was measured by the rate of reduction in installations of a software for suspicious scenarios relative to benign scenarios. Nonetheless, the rate of cancelling suspicious dialogues is affected by other factors such as a lack of willingness to fulfil the request (e.g. update a plugin) or a lack of the feeling of vulnerability, if users could detect that warnings were all fake. The results showed that although inhibitive attractors resulted in a higher reduction in the installation rates compared to the control group, warnings with these types of attractors were more time-consuming to handle for participants (Bravo-Lillo et al. 2013). The swiping and type attractors took the most time.

Karegar et al. (2018b) studied users recall of personal information shared via permission dialogues using checkboxes. They also investigated the effect of previewing the selected personal data on enhancing users attention before they give their consent. Karegar et al. (2018b) did not, however, compare the effectiveness of permission dialogues utilising checkboxes with any other types of interaction techniques.

In another work, Karegar et al. (2018a) adapted the DAD to fit the context of identity providers for selecting the personal information to be shared with the service provider using Facebook single sign-on. Their study shows that using DAD significantly helped users to recall the information they share with services using their Facebook account and reduced the user's level of uncertainty. Karegar et al. (2018a) compared their proposed solution, using DAD to select personal information to be shared, with the mock-up of the permission dialogues of Facebook in which all requested personal information was pre-selected by default with the opportunity to be opted out at the second layer. Therefore, more investigation is still required for the direct comparison of checkboxes and other interaction techniques like the DAD in the context of consent forms.

Utilising interaction techniques to engage users has its own challenges: there is a risk of over-burdening the users. The example from healthcare, briefly referred in Section 1, Assale, Barbero, and Cabitza (2019), is not easy to generalise to other contexts because the researchers designed a rather thorough dialogue window, where patients could provide their emotions in relation to various parts of the consent text and be supported by further information accordingly. This probably would be too complicated for everyday use. In fact, the researchers report that even healthcare workers are hesitant:

> an electronic informed consent that is aimed at creating more (not fewer) opportunities of interaction between patients and care givers was seen as practically incompatible with their agenda, and to require additional time that cannot be expected and planned in the current hospital workflow. (Assale, Barbero, and Cabitza 2019, 614–615)

None of the previous works, which tried to increase user attention to, and understanding of, the consent form contents, investigated or compared the usability of alternative interaction techniques, i.e. design patterns, to actively involve users in the consent forms, or for the data selection, to achieve informed consent, on mobile devices. Given the prevalence of mobile devices, it is more important than ever that we have solutions for people to give their informed consent in the mobile interface context. Therefore, in this work, motivated by the theoretical model of interactivity effects (Sundar 2007) and to address the gap in the literature regarding the effects of different interaction techniques on users' experience we investigate alternative design solutions for mobile phones to actively engage users in consent forms. We compare different alternatives in terms of the usability and user awareness of their personal data flow. We expect that these results will provide insights for designers, and inspire them to improve on the current methods to elicit informed consent in permission dialogues and consent forms on smartphones. Table 1 gives an overview of research discussed in this section and places our study in the context of the earlier work.

3. Methodology and study design

The main purpose of the user study conducted in this paper is to compare different design solutions serving as affirmative actions on permission dialogues of IdPs in terms of their effectiveness to help users to be aware of the information they share, users' satisfaction, and efficiency. To achieve our goal, we designed a between-subject user study with 3 groups of 20 people. As individuals were recruited to the study, they were randomly assigned to one of three groups: either the checkbox, Drag and Drop or swiping group. User tests were conducted individually, one-to-one with the researcher, and the test used depended on the group to which the individual was assigned. For each group, the participant (user) experiences a specific way of engagement in the content of a permission dialogue of an IdP via an affirmative action (see Section 4 for a detailed description of each method of engagement). In this section, we first describe the study design. Then we outline the recruitment and demographics and finally, we explain our evaluation methods.

Table 1. Overview of research on interaction techniques to engage users' attention with content.

Study	Context	Type	Measurement method for user attention	Results		
				Effectiveness: User attention	Efficiency: Time	Satisfaction: SUS score
Bravo-Lillo et al. (2013): Swipe and type inhibitive attractors	Security warnings: Desktop	Online exp.	Rate of reduced installations in suspicious relative to benign scenarios	Inhibitive attractors resulted in a higher reduction in the installation rates	Inhibitive attractors take more time	—
Wang, Grossklags, and Xu (2013): Pre-selected Checkboxes	Permission dialogue for IdP consent: Desktop	Online exp.	Counted data items released and opt-out actions	Users of checkbox-enabled interfaces release less information and opt out from some data collection	—	—
Sundar et al. (2014): Click, Slide, Zoom, Hover, Drag, and Flip	Informational website: Desktop	Lab. exp.	Recall of website information	Improved content recall depending on interaction technique	—	User assessment and power usage correlated in various methods
Karegar et al. (2018b): Checkbox, Confirm screen plus checkbox	Permission dialogue for IdP consent: Mobile	Lab. exp.	Recall of personal information shared	Confirmation screen helps improve information recall	Reports Mean time to handle checkbox interfaces. Implies longer time for confirmation and checkboxes	Good SUS scores for both types of interfaces
Karegar et al. (2018a): DAD and pre-selected checkboxes	Permission dialogue for IdP consent: Desktop	Lab. exp.	Recall of personal information shared	DAD helps users recall information they share and reduces their uncertainty	DAD interfaces are more time-consuming	DAD interfaces have lower SUS values, within the acceptable range
CURRENT: DAD, Swipe, Checkbox	Permission dialogue for IdP consent: Mobile	Lab. exp.	Recall of personal information shared	DAD and swipe give better Recall values	Checkboxes take less time than Swipe or DAD. Swipe and DAD have almost the same completion time	All earn good SUS scores: DAD scores highest SUS; Swipe scores lowest. SUS score is independent of age

3.1. Study design

We implemented our prototypes using Axure prototyping tool[2] and tested our prototypes with users on a Samsung S6 phone. Every session for each individual participant included an introduction by the moderator and consent giving by the participant, the completion of the authorisation task, answering the post-test questionnaire, as well as debriefing and compensation. Figure 1 provides an overview of the study design and collected information.

Introduction session: The moderator welcomed and thanked the participant. The moderator then introduced the study, which provided the participant with information about the persona and the task that needed to be completed. Participants role-played a persona that wished to subscribe on a website in order to purchase a product. In order to subscribe on the website the participants were required to select an IdP, the CREDENTIAL Wallet IdP in our study, for which the given persona had an account. The persona's username and password of the IdP account were provided to participants during the introductory session. All of the participants role-played the same persona and had a standardised experience. The introduction session finished with signing the consent form for the study. In the consent form, among other information, participants were informed about using a screen-recorder software on the mobile device used in the study. Before their participation, participants were requested to read the consent form for the study and sign it if they agreed to continue. More information about the research consent form and ethical consideration are reported in Section 3.2.

Authorisation task: The mock-up of a fictitious website, the PhotoHex website, that was designed for the study, and for which participants were asked to subscribe, was accessible via a laptop during the test. On visiting the website, participants selected the IdP (CREDENTIAL Wallet) to subscribe to the website. Then, they entered the username and password of the persona's account and were instructed to use the mobile phone given to them in the study to open the mobile app of the IdP (the CREDENTIAL Wallet app), and so proceed to complete the authorisation task.

Using the mobile phone, participants clicked on the icon of the IdP app (the CREDENTIAL Wallet app) to open it and sign into the app, by pretending to scan their fingerprint by clicking on a specific icon on the device screen. The methods to sign into the IdP app include entering a pre-determined pincode or scan a fingerprint. For the study, we assumed the persona chose to scan a fingerprint to unlock/sign into the app the first time she downloaded the app on her phone and created the account. However, participants' preferences for the method to unlock/sign in to the app and their understanding of the personal data flow used for unlocking/signing into the app is out of scope of this paper. A full report of users' understanding of fingerprint used in the context of IdPs can be found in Karegar, Pettersson, and Fischer-Hübner (2018).

After unlocking/signing into the app, participants handled the authorisation dialogues, i.e. they selected the personal data to be shared by an affirmative action based on the group to which they were assigned. In all prototypes, the authorisation dialogues requested full name, email address, and date of birth as mandatory information; and a profile photo and personal interests as optional information. After selecting the information types, participants continued by accepting the service provider's request (the request of the fictitious website in the study) and returned to the laptop to see the confirmation message on the website confirming that they were subscribed.

Questionnaire: The post-test questionnaire included demographic data (age, gender, education level), System Usability Scale (SUS) questions (Brooke 2013), IUIPC questions for control, awareness and collection to measure the level of users' information privacy concerns (Malhotra, Kim, and Agarwal 2004) as well as some questions to recall the information that users shared, and for the data processing purposes requested, with the service provider from their IdP accounts. Section 3.2 provides more details on demographics and participants' IUIPC scores. More details about SUS and IUIPC questionnaires and methods to measure usability and awareness which we used in our study are elaborated in Section 3.3.

Closing phase: After participants answered the questions in the post-test questionnaire, the moderator debriefed them about the study and gave them the opportunity to ask their questions, if they had any. Moreover, each participant was compensated with a coffee coupon for the university canteen.

3.2. Ethics, recruitment, and demographics

We complied with the necessary steps to adhere to the Swedish Research Council's principles of ethical research in our study (Vetenskapsrådet 2002). We obtained informed consent, did not use sensitive or actual data without anonymisation. We collected Age, Gender, and Education level anonymously. Furthermore, we used a persona for the authorisation task to avoid using participants' personal data in the prototype. The task and questionnaire were completed 'anonymously' using the

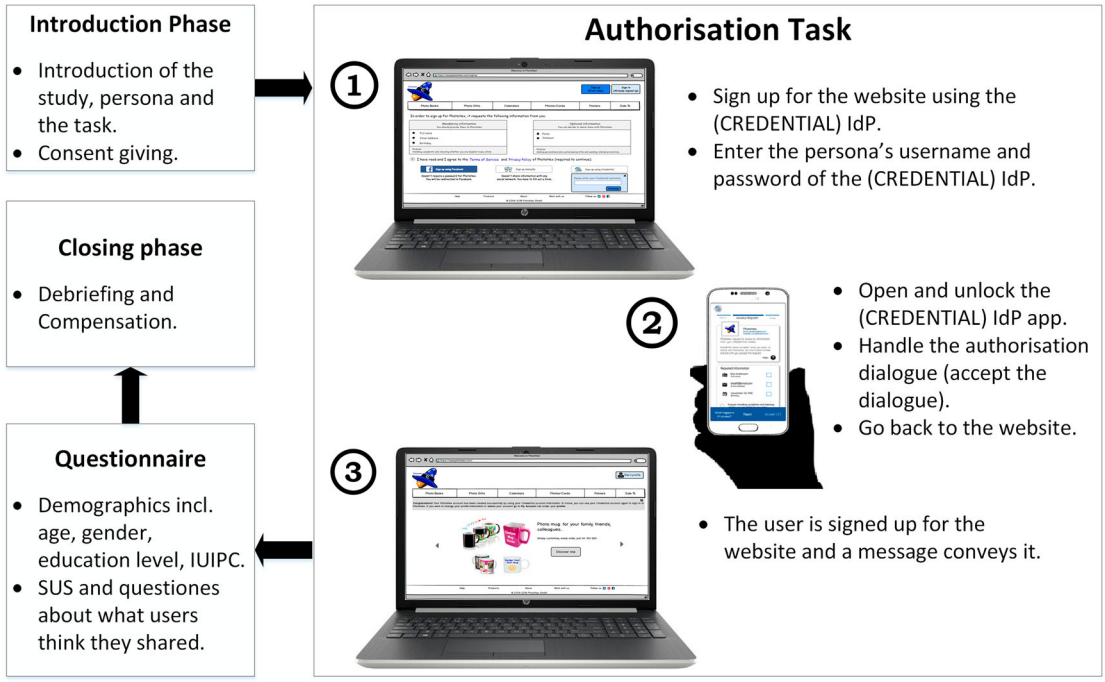

Figure 1. The flow of our study design.

persona. Participants were debriefed and compensated at the end of the study.

As we are interested in gauging the impact of designs rather than seeing the effect for different groups of the society, all participants were recruited at our university. There is some variation in Education level, but in our analysis afterwards the Educational level of the participants has no correlation with performance in the task. We recruited 60 participants to have three groups of equal size, 20, as this size is shown useful in earlier studies (Karegar et al. 2018b). People were approached and asked to participate for a small compensation (the coffee coupon mentioned in Section 3.1). Participants were randomly assigned to one of three groups of the study.

Table 2 shows our participants' demographic profiles. In total, we had 60 participants, of whom 18 were female, 41 were male, and one preferred not to reveal the gender. The Mean Age of participants is 25.8 years old, and 51 (85%) of the participants belong to the age group 19–29 years old. We assess that our participants are rather concerned about their information privacy because of their relatively high scores (above 50) with the IUIPC test. For each group of 20, the Mean IUIPC score is over 50, out of a potential maximum of 70, i.e. each group scored over 70% for their Mean IUIPC score. The overall IUIPC score for the 60 participants is: Mean = 55.78, Min = 34, Max = 70. More details on IUIPC scores are reported in Table 2.

Table 2. Demographic information.

Demographic information	Swiping (n=20)	DAD (n=20)	Checkbox (n=20)
Gender			
Female	9	5	4
Male	11	15	15
No answer	0	0	1
Age			
19–29	19	18	14
30–39	1	1	5
40–49	0	0	1
50–70	0	1	0
Mean	24.7	25.4	27.3
Educational level			
Secondary school degree	5	3	4
Bachelor level	9	7	7
Master level	6	10	9
IUIPC for control, awareness, and collection			
Minimum	34.00	37.00	43.00
Maximum	70.00	69.00	70.00
Mean	51.55	56.40	59.40
Std. deviation	10.01	9.14	7.52

3.3. Evaluation method

The purpose, as outlined in Section 1, is to investigate the impact of interaction paradigms, i.e. a selection of design concepts, for data selection and active engagement of users on usability and user awareness of data transactions. In this section, we describe the methods we used to compare the alternative interaction paradigms in terms of their effectiveness to help users to be aware of the information they share, users' satisfaction, and efficiency. We do this by reference to standards for usability metrics. In addition, we also explain how we

evaluated participants' information privacy concerns to investigate if a users privacy concern level has any impact on the awareness of data transaction.

Usability metrics: Before measuring the usability of a prototype, it is required to define usability and how to measure it. Usability is defined as 'the extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use' in ISO 9241-11:2018, Section 3.1.1 (ISO 2018).

Effectiveness is defined as the 'accuracy and completeness with which users achieve specified goals' (ISO 2018, sec. 3.1.12). We measure effectiveness by quantifying the accuracy of doing the tasks and the recall of information. In other words, we measure if users have difficulties or interruptions while doing the tasks and how much information users can recall after using the UIs.

There are a few methods for measuring users' awareness of data transactions that are consistently used in the literature related to permission dialogues. Most of the research relies on the information that users' remember as an indication of their awareness of data transactions (Bauer et al. 2013; Egelman 2013; Ronen et al. 2013; Karegar et al. 2018a, 2018b) while some of the research uses eye tracking (Javed and Shehab 2016) or both (Javed and Shehab 2017) to measure users' attention towards the dialogues and their awareness of the information that they share. In the context of IdPs, researchers specifically target the information types rather than the data transactions as a whole (Bauer et al. 2013; Egelman 2013; Ronen et al. 2013). Ronen et al. (2013) explore how well users can remember personal data transferred from their IdP accounts to service providers by asking participants to list the information types that they thought were transferred. The participants' responses are then compared with the actual information types transferred to service providers using precision and recall measurements. *Precision*, as defined by Ronen et al. (2013) is the ratio between the number of information types a user lists correctly and the total number of information types the user lists. On the other hand, *recall* is the ratio between the number of information types a user lists correctly and the number of information types that are actually transferred to the service provider (Ronen et al. 2013).

In our user studies, participants are exposed to a table of fourteen data types in the post-test questionnaire, and for each data type they select to indicate if they share the data type with the service provider from the IdP account or not. Participants also have an option to indicate if they 'Cannot recall'. In other words, participants have three options to select for each data type: (i) shared, (ii) not shared, and (iii) not sure. We apply the metrics used in Karegar et al. (2018b) which are the extended version of the metrics (Ronen et al. 2013) used and we calculate precision as: the ratio between the information that the participant correctly lists as shared, or not shared, and all the information listed as shared, or not shared. Recall is calculated as: the ratio between the information that the participant correctly lists as shared, and the information that is actually shared. Including *not sure* as a possible answer for each data type helps to have more reliable *shared* and *not shared* answers. Moreover, having the *not sure* option allows us the opportunity to calculate the self-expressed uncertainty level for each participant and examine which design helps participants to be more certain about the information they share and do not share.

However, it is not enough to know the information that the service provider requested from the IdP that is conveyed through the permission dialogues. For example, with the widespread use of fingerprint sensors on mobile devices to unlock the phone, authenticate to apps, and confirm purchases, it is important to ensure that people understand that fingerprint data is processed and stored locally on their devices, under their control and is not sent to the service providers (Karegar, Pettersson, and Fischer-Hübner 2018). When people do not understand how the fingerprint data are processed it can be a barrier to the adoption of fingerprint sensors by users (Bhagavatula et al. 2015). Consequently, not only is it crucial to know the information that is *shared* with the service provider from the IdP, it also matters that users know the information, specifically the sensitive information, that is not shared with the service provider.

Efficiency is defined as 'resources used in relation to the results achieved' (ISO 2018, sec. 3.1.13). We measure efficiency by timing participants while they were completing the authorisation tasks. We time participants from the moment they start to type the persona's username and password into the website, to the moment when they are enrolled and receive a confirmation message on the website.

Finally, satisfaction is 'extent to which the user's physical, cognitive and emotional responses that result from the use of a system, product or service meet the users needs and expectations' (ISO 2018, sec. 3.1.14). We measure overall usability and satisfaction by using the standard SUS questionnaire. The SUS questionnaire provides lightweight, ten five-point Likert scale questions, and subjective feedback from users (Brooke 2013) which is a robust approach even when testing with a small number of participants (Albert and Tullis 2013). The 10 questions lead to a SUS score between 0 and 100. Bangor, Kortum, and Miller (2009) map descriptive adjectives to a range of SUS scores and report that a SUS

score below '50' is unacceptable, over '50' is OK, over '70' is acceptable, and a score of '85' is 'Excellent'. Ruoti and Seamons (2016) propose that usability studies concerning authentication systems should use a standard metric like SUS to provide stakeholders with the opportunity to compare systems in a standard framework and choose the system that fits the best. Indeed, Ruoti, Roberts, and Seamons (2015) recommend all new authentication systems should achieve an SUS score of at least 70 before the system is considered as a new proposal to replace current practices. We use SUS to evaluate our prototypes which are designed in the context of authentication systems.

The collected results for SUS, efficiency, and effectiveness are reported in Section 5.

Level of information privacy concerns: In the questionnaire, we used IUIPC to investigate if a user's privacy concern level has any impact on the usability and awareness of data transaction by looking at correlations between the IUIPC scores and user awareness scores, i.e. recall, precision and uncertainty, of data transactions. Therefore, the widely used IUIPC constructed by Malhotra, Kim, and Agarwal (2004) is adopted in our study which is developed to measure peoples general concerns about organisations information handling practices. The model claims to explain a large amount of variance in behavioural intention and thus serves as a useful tool to analyse users' reactions to different types of privacy threats. The IUIPC scale defines multiple groups of privacy concern including (i) dimensions of control of personal information, (ii) collection of personal information, and (iii) awareness of information privacy practices. These groups have ten statements in total: three for control, four for collection, and three for awareness, and use 7-point Likert scales that range from 1, Strongly Disagree, to 7, Strongly Agree. Based on the responses, a privacy score between 10 and 70 for each participant is generated. The higher their privacy score, the more concerned participants are about their privacy. Table 2 summarises the IUIPC scores for participants in each of the test groups.

4. Design of the consent dialogues

In this work, we design three alternative types of interaction, i.e. actions that indicate users' consent to processing their personal data they select on permission dialogues, based on current practices on websites and research literature. This section describes the common layout of all three designs and then presents our three proposed modes of selection namely (i) Drag and Drop, see Figure 2, (ii) swiping, see Figure 3, and (iii) checkboxes, see Figure 4.

General layout: At the outset, it is important to develop a hierarchy of information and determine the information to be displayed and at which positions (Cooper, Reimann, and Cronin 2007) because the layout of items is an important aspect to facilitate users' comprehension (Patrick and Kenny 2003). To create a visual hierarchy for users, while presenting clear actions, we used card-based interaction model which is widely utilised in the design of various websites and mobile applications. Aggregation of many individual pieces of content can be presented in the form of cards. Cards are rectangles containing text, images, and functions related to one subject. In our proposed prototypes, cards are used to separate information according to their content: (i) a box presenting information about the identity of the service provider making the request, (ii) a box presenting the mandatory data types with the general purpose of collecting these items, and (iii) a box for the optional data types accompanied with the general purpose of collecting optional information. According to GDPR (The European Parliament and the Council of the European Union 2016), consent should be unambiguous, freely given, specific, and informed. For a consent to be informed, pursuant to Article 13 (1) GDPR, people should at least be made aware of the personal data that will be collected and processed, by whom, and for which purposes. For example, is the information going to be used for targeted advertising or will the service provider use the information to deliver services to the user?

A sticky footer is included in the design at the end of the application screen to give users the option to cancel or accept the request at any time. To provide better visual assistance for users about the specific information, and the number of items they select, the number of selected items is shown on the sticky footer.

Icons: Icons can be used to display logical arrangements of the interface to ensure awareness in privacy systems (Patrick and Kenny 2003). Requested information in our proposed user interfaces are presented as icons. Each icon is accompanied by a label denoting the information that the icon represents and the exact piece of personal information from users' IdP account that is associated with the icon. As icons may be interpreted differently by different users, we used the results of a mini-survey before presenting participants with the information represented in icons. We conducted a mini-survey in which for each piece of information we asked people to select the most relevant icon among a list. The depicted

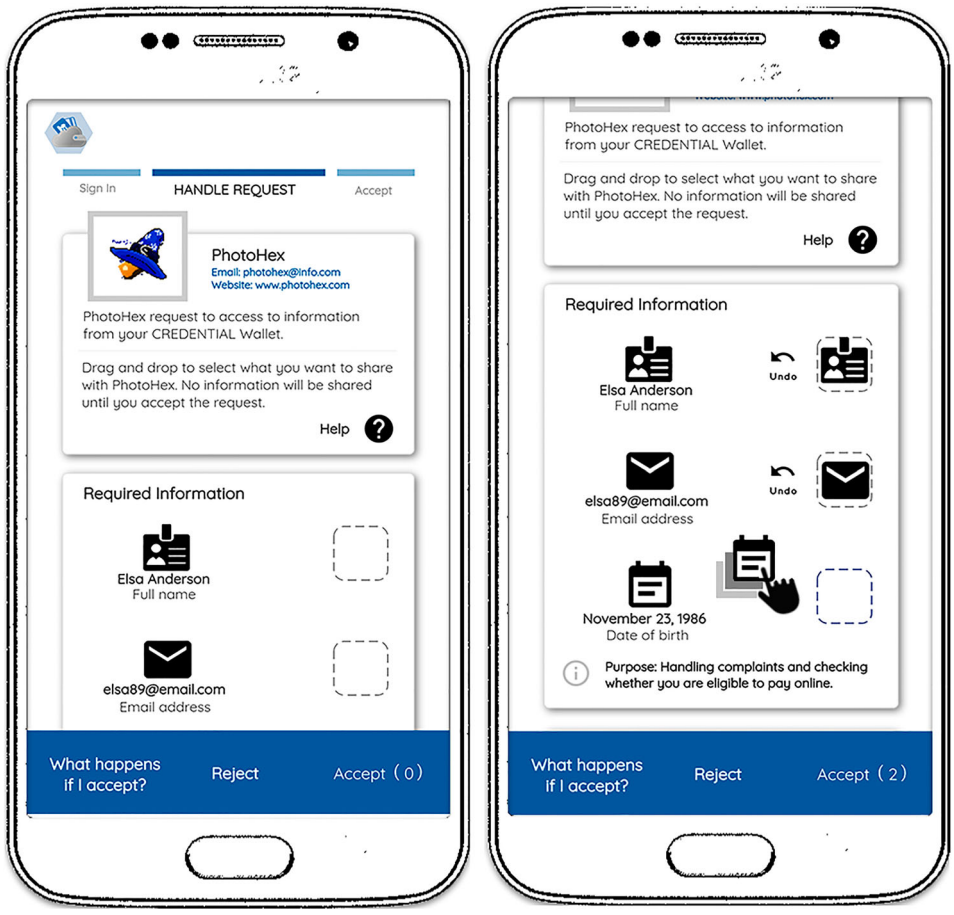

Figure 2. 'Drag and Drop' prototype. Left: before data selection. Right: after two data selections and a third being dragged towards the empty square.

Note: The screen is scrolled down in the right image.

icons in our design are derived from the results of this exercise.

Tutorial: Tutorials are important in order to make users aware, feel in control and comprehend how information is handled (Patrick and Kenny 2003) as participants who use a system without a tutorial may have a more difficult time completing the tasks (Ruoti and Seamons 2016). For each of the proposed design solutions we provide interactive tutorial pages by which users are guided as to how they can complete the action, i.e. choose among the presented data types, see Figure 5 as an example of a tutorial we provided to users. DAD and swiping are new concepts for users to be used in the context of permission dialogues. Therefore, interactive graphical tutorials should be provided, at least, upon request which can abate the primary confusion about how users should select their desired piece of information. In our study, the tutorials were shown to users if they clicked on the *Help* icon (depicted with a question mark, see Figure 2 as an example) in each of the prototypes.

4.1. Drag and drop

Pettersson et al. (2005) first proposed the DAD concept to be used in consent forms to avoid users' automated behaviours that stemmed from dialogue boxes with two alternatives of 'OK' and 'Cancel'. They propose the DAD concept to address the problem of habituation to which Just-In-Time-Click-Through Agreements suggested in the PISA project (Patrick and Kenny 2003) (JITCTAs) are vulnerable. The PISA project is cited in many works over the past two decades (e.g. Kobsa and Teltzrow 2005; Morrison, McMillan, and Chalmers 2014; Gluck et al. 2016). Pettersson et al. (2005) propose consent forms utilising DAD in which users have to drag the graphical items of personal information and drop them to a suitable, desired receiver of that personal information among a number of possible receivers of data. Karegar et al. (2018a) utilised DAD in the context of authorisation dialogues of IdPs on desktops and reported about the efficiency of the method, effectiveness in helping users to pay more attention to the information they share and their satisfaction. The

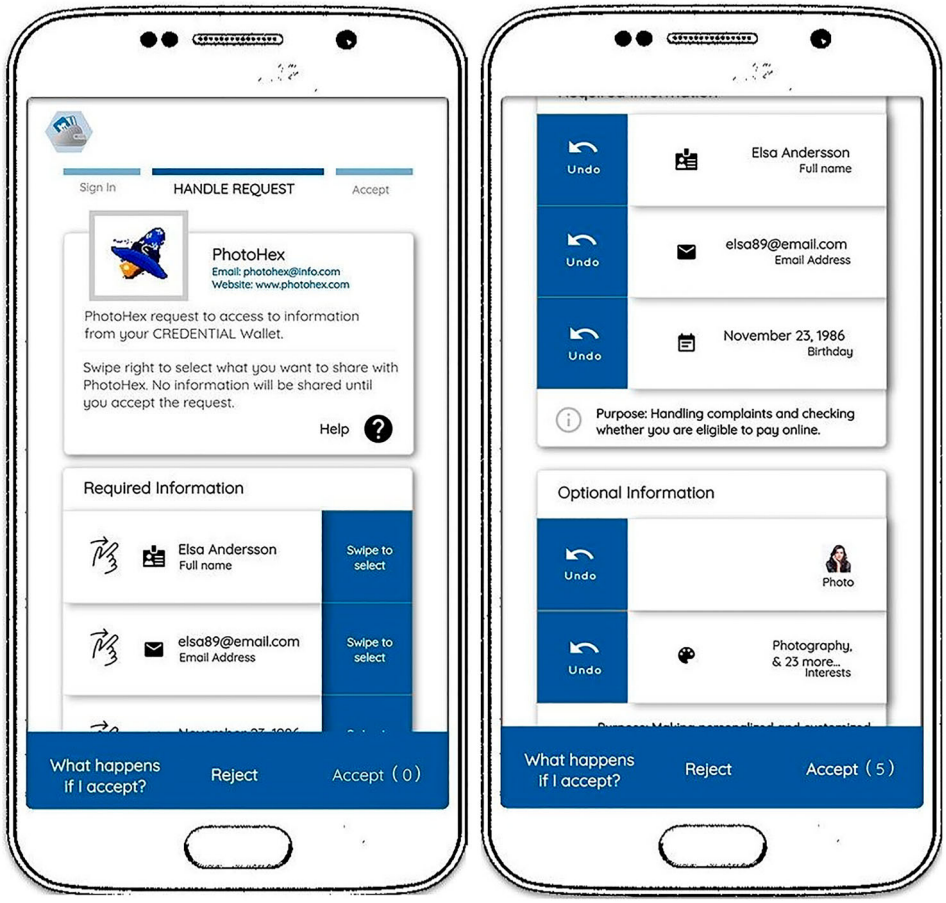

Figure 3. 'Swiping' prototype. Left: before data selection. Right: after data selection using swiping.
Note: The screen is scrolled down in the right image.

DAD approach, however, has yet to be tested on mobile devices.

In our proposed solution for DAD, the user must drag the appropriate icon and drop it to a closed drop zone specific for that icon in order to select a piece of personal information to be processed, i.e. to share with the service provider, as depicted in Figure 2. Once selected, an *undo* text with an icon is available to users. Clicking on the icon will undo the action previously selected.

4.2. Swiping

Smartphones open up a new medium for users to learn and anticipate different methods to initiate functions (Hoekman 2010), such as tapping, pinching, spreading, and swiping which cannot be achieved on desktop computers without touch screen monitors. Among the methods, swiping mimics the gesture of flicking something off a physical surface (Murray 2011). Swiping gestures are utilised in various mobile apps to fulfil a variety of goals. Some research shows the positive effect of swiping interaction on user experience in different contexts. For example, Choi, Kirshner, and Wu (2016) compare swipe-based shopping applications with traditional scroll-based ones and shows that the swiping interface leads to greater cognitive absorption and playfulness in shopping applications. In another study, Dou and Sundar (2016) show that the addition of swiping technique to a tap-only mobile website positively affects behavioural intentions to use the website.

There is no indication on most app interfaces to show if swiping gesture is active and of the functionality it may provide. Users may try different gestures on various elements on an app to explore the actions that they can achieve. For example, swiping right-to-left and left-to-right are used in Gmail app to delete emails while swiping left-to-write in Telegram app is used to reply to a message. Thus, swiping functionality and its existence may not be immediately obvious to users. To make the functionality more explicit, some signifiers, such as arrows and icons, can be adopted to provide clearer signals about the operations available (Norman 2013).

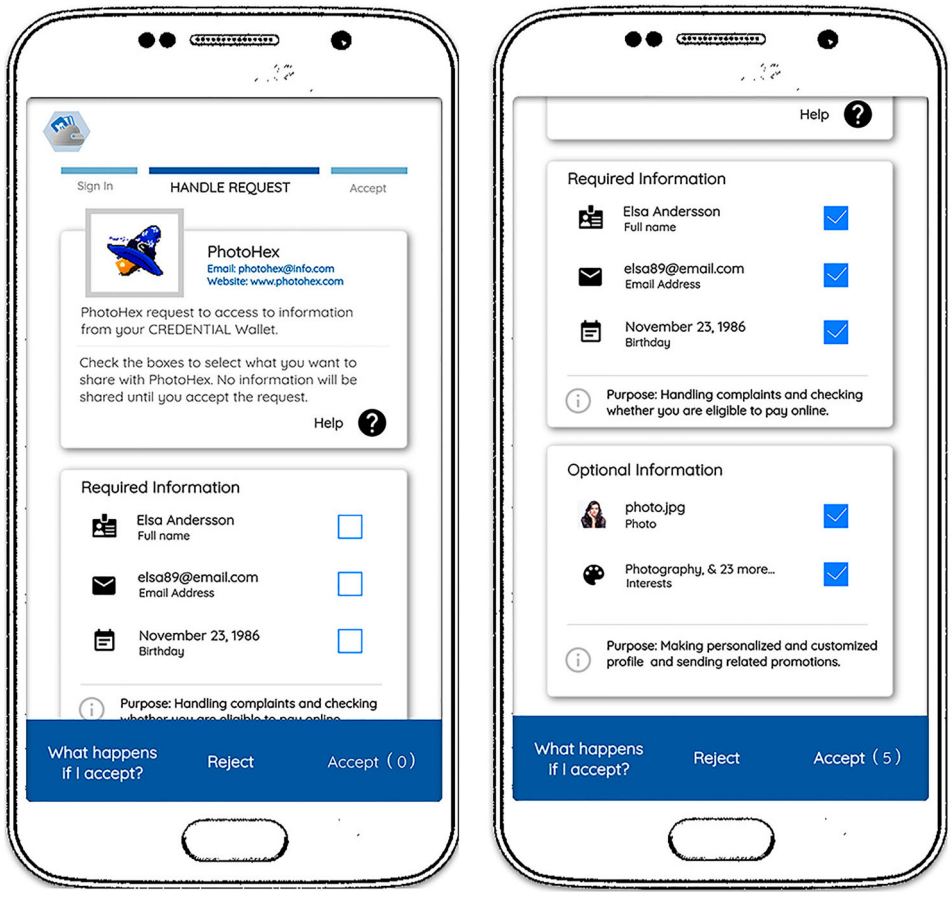

Figure 4. 'Checkbox' prototype. Left: before data selection. Right: after data selection using checkboxes.
Note: The screen is scrolled down in the right image.

In our design solution, we utilise the swiping gesture to create a sense of completion and show a clear example of a before-and-after scenario for selecting items. In order to explain the functionality of selecting information a swiping icon consisting of an emoji of a pointing hand and an arrow with its head towards the right direction is designed, see Figure 3. The icon shows the direction of movement which is accompanied with a text presented on a contrasting background colour. The text conveys to users that they can swipe to select a data item, and helps them to complete the selection task.

4.3. Checkbox

The use of checkboxes on websites to indicate the user's acceptance of terms and conditions or privacy policies, is common practices nowadays. Wang, Grossklags, and Xu (2013) proposed to use checkboxes on Facebook authorisation dialogues at a time when Facebook interfaces did not provide users with choices. Karegar et al. (2018b) used checkboxes in an app interface for an IdP and evaluated users' understanding and awareness of their personal data flow. The results of Karegar et al. (2018b) study show that participants prefer to select mandatory information themselves rather than have the mandatory information pre-selected. Furthermore, although the participants are not completely unaware of their data flow and the information they share with the service provider from their IdP account (Karegar et al. 2018b), their awareness and attention towards their personal data sharing could be improved. To this effect, in our study we include prototypes that utilise checkboxes, see Figure 4, to serve as a control group to test if there are design solutions that outperform checkboxes in users' satisfaction, efficiency, and effectiveness.

5. Results

We compare alternative design solutions for affirmative actions on permission dialogues in terms of their efficiency, satisfaction, and effectiveness to help users to be aware of the information they share. We compare the designs based on both the measures and observations, as follows: (i) we time participants when they perform their tasks, (ii) measure the SUS values, (iii)

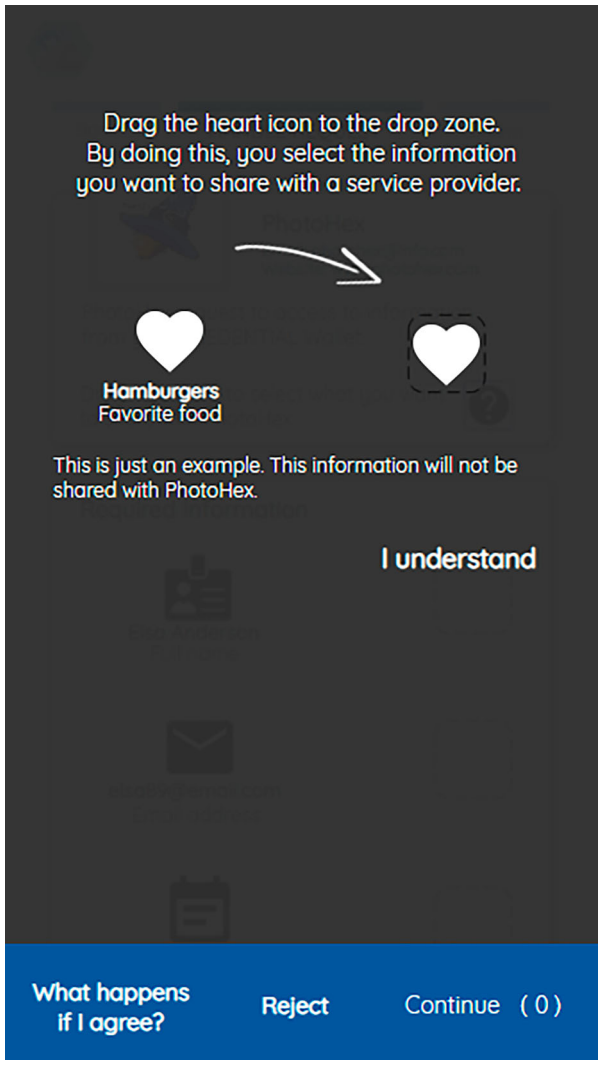

Figure 5. An example of a tutorial screen in our study, the DAD tutorial, provided upon request when a user clicks on the help icon.

observe if they encounter any severe difficulties, and (iv) measure the extent to which users are aware of personal information they share with the service provider from the IdP account. In this section, we first report the results of our measurements.

Efficiency: Table 3 shows the time it took participants to perform the task for each design solution. Design patterns affect the time it takes to complete the tasks. Overall, participants take less time to select the data types when using checkboxes. The Mean time for completing the tasks while using swiping and DAD is almost the same, but more time is needed than for using checkboxes. Whether the quickness of the checkbox method affects the users' awareness and attention, or not, remains to be investigated. For example, users' awareness could be compared while using alternative designs when deciding to share their personal data.

Table 3. Time to complete the authorisation task.

Time in seconds	Swiping	DAD	Checkbox
Min	42	51	43
Max	284	592	275
Mean	132	129	93
Standard deviation (SD)	68	114	55

Effectiveness and awareness: In terms of task completion, all participants across the three experimental groups managed to complete the authorisation task without any major interruption or difficulty.

As explained in Section 3.3, we measure the effectiveness of the alternative design solutions to help users to be aware of the information they share with the service provider by measuring *Recall*, *Precision*, and *Uncertainty* levels. Table 4 shows the Precision, Recall, and Uncertainty scores measured for the alternative design solutions. The Mean Recall values for swiping and DAD are better than for the checkbox design, although statistical significance is not demonstrated in this sample of 20 for each method. The Mean Uncertainty level is lowest for checkboxes compared to DAD and swiping. The Mean Precision values for the three methods are very similar.

In total, 14 data types are presented in a list to the participants in the post-test questionnaire, 5 of which are requested in the prototypes as mandatory and/or optional information. Two of the data types in the list are *fingerprint pattern* and *age*. A question in the post-test questionnaire with regard to where the fingerprint pattern is processed reveals that users have an incorrect mental model of fingerprint processing. Many users believe that their fingerprint pattern is shared with the identity provider and the service provider. Furthermore, although *age* was not directly requested in the permission dialogues, *age* was implicitly shared with the service provider since the date of birth was requested

Table 4. Measuring awareness: precision, recall, and uncertainty levels.

Value	Swiping	DAD	Checkbox
Precision			
Min.	0.63	0.58	0.50
Max.	1.00	1.00	1.00
Mean	0.85	0.88	0.89
St. dev.	0.14	0.09	0.15
Recall			
Min.	0.60	0.60	0.20
Max.	1.00	1.00	1.00
Mean	0.93	0.92	0.84
St. dev.	0.13	0.13	0.24
Uncertainty			
Min.	0.00	0.00	0.00
Max.	0.83	0.58	0.50
Mean	0.20	0.15	0.10
St. dev.	0.22	0.16	0.15

as mandatory information. Several participants remember that they share their date of birth but they mistakenly say that they are not sharing their age. Considering the misconception about the fingerprint processing and lack of critical thinking about the *age* data types from participants, we exclude fingerprint pattern and age in our calculation of Precision, Recall, and Uncertainty values. The reason for this omission is because the wrong answers to those data types are affected by users' misconceptions more than being affected by the design solutions.

Bauer et al. (2013) state in their work that users have some preconceptions of personal information shared in the context of IdPs, regardless of the permission dialogues shown to them. Asking users to recall what they shared to measure their awareness and attention does not necessarily show the exact effectiveness of dialogues in catching users' attention to the information they share with the services. In the questionnaire, when they are requested to Recall the information that they share and do not share, the preconceptions about data types shared with the service provider may influence their answers. Therefore, other methods to triangulate the measurements for awareness and attention could help in this context. For example, the eye tracker can be used to check if, and for how long, users look at important items in permission dialogues.

In the post-test questionnaire, we ask participants to indicate the data processing purposes for which the service provider could use their personal information. We provided a general data processing purpose for mandatory information and a general data processing purpose when requesting the optional information. Very few participants ($n \leq 7$) gave an acceptable answer when recalling the purposes given in the prototypes. It seems users were more focused on data collection than on reading the data processing purposes and the conditions of the requested permissions.

Satisfaction: The results of SUS values calculated for the different groups are reported in Table 5. The DAD achieved the highest score and the swiping design the lowest scores. Apparently, while both are within the *Good* range, according to Bangor, Kortum, and Miller (2009), different design patterns have a notable impact on the perceived usability.

Table 5. SUS values for different design solutions.

SUS	Swiping	DAD	Checkbox
Min	42.50	55.00	52.50
Max	92.50	97.50	97.50
Mean	72.63	81.00	79.25
St. dev.	13.02	9.30	10.42

6. Analysis and discussion

Comparing design solutions: Karegar et al. (2018b), based on the results of their study, report that a confirmation page can be utilised as a way to slow users down without obstructing them and to help them to be more attentive. Instead of using the confirmation screen to slow users down a little and have them reflect on the information they select to share, we decided to use the time actively and engage users in the dialogues. The results show that, with almost the same precision, DAD and swiping give better Recall values, but are, in general, more time-consuming. The improved Recall values may have been achieved because of the avoidance of automated behaviours (Pettersson et al. 2005) compared to checkboxes which are common practices on websites or different software applications to show users' acceptance of the Terms and Conditions. However, the robustness of methods against habituation should be tested. Moreover, the time to complete the task and the Recall values are not significantly correlated with each other. In other words, spending more time on the dialogues will not necessarily result in better or worse recalling of personal information shared. Direct methods for measuring attention such using eye trackers could have helped in this regard.

DAD design takes 36 seconds more time, on average, for participants to complete the authorisation task, than for checkboxes (Table 3). However, DAD helps them to recall better the information they shared with almost the same precision. Three participants who experienced the DAD design thought at the first glance that the drop zones were checkboxes. In general, the unfamiliarity with the DAD design did not affect the satisfaction as the DAD design received the highest SUS score among all the designs in our study.

Among all three designs, swiping received the lowest SUS score on average and highest time to finish the task. During the study, approximately half of the participants (n=11) who experienced the swiping prototype got a little bit confused as to how to proceed the first time they saw the authorisation dialogue, which could explain the reason for the lowest SUS score and the longest time to handle the swiping prototype among other design solutions, see Table 5. Four participants thought that they were supposed to swipe from right to left instead of the intended motion which was left to right. Nonetheless, all 20 managed to complete the task, and just 3 clicked on the help icon and used the tutorial. The swiping gesture activated in different mobile apps provide varied functionalities based on the direction of the movement, i.e. users will experience different results if they swipe to the right or to the left. Although the functionality of

the swiping gesture in mobile apps may have been described in their tutorials (if available), our observations suggest that it would be more beneficial for users to have the tutorials shown by default to them for the first time they use the apps that utilise specific movement gestures.

Rather than specific deficiencies in the design of DAD and swiping, i.e. confusion about the direction of swiping and the drop zone of DAD that slow down users, we observe a common problem in all the three designs tested: a lack of strong signifiers for mandatory information. Although we separated the mandatory and optional information in the design solutions, it did not help to prevent participants from trying to skip the selection of some of the mandatory information. Some participants tried to proceed without selecting all mandatory information, which was not possible; they did not notice that the *Continue* button was deactivated. For example, one participant in the DAD group who took the longest time to complete the task of all other participants failed to notice, for quite a long time, that the date of birth needed to be selected in order to proceed, see Table 3 for Max. in DAD. The problem could have been avoided with a more prominent visualisation of the required information and providing error messages besides deactivation of the *Continue* button.

In sum, using stronger signifiers to distinguish between mandatory steps and optional ones to complete a task and having the tutorials open by default for the first time users reach the authorisation dialogues, that utilise new design patterns such as DAD and swiping, could help to avoid the confusion and decrease the time for data selection.

Correlation between demographics, usability, and awareness: Several studies discuss the correlation between usability and basic demographics such as gender and age (Sears, Jacko, and Dubach 2000; Sindhuja and Ghosh Dastidar 2009). In this study, we also examined the correlation between Age, Education, Gender, IUIPC scores, as demographics, and usability (i.e. Time and SUS values) and awareness values (i.e. Precision, Recall, and Uncertainty) to be able to explain the effects of our designs on different people. We find no statistically significant correlation in our sample of 60 between Gender, or Education, and usability and awareness values. Furthermore, there is no statistically significant association between Age, SUS and awareness values in our sample. However, there is a significant positive relationship ($p \leq .01$) between the time taken to complete the authorisation task and the Age group (under 30 years old; over 30 years old) based on Pearsons correlation (0.361). Participants under 30 years old completed the task in less than 100s while people over 30 needed more time. Interestingly, the time to complete the task is not significantly correlated with Recall values.

Finally, we examined the relationship between IUIPC levels and Recall and Uncertainty values. Although not significantly correlated with Recall values, IUIPC scores are significantly correlated with Uncertainty scores ($p \leq .05$). Pearson's Correlation value is $= -0.256$. Our data shows that the respondents with higher IUIPC scores had lower Uncertainty scores, which means that they were more confident about the information they shared and not shared with the service provider, i.e. providing less *not sure* answers.

Implications of our results: The results of our study shed lights on the future design of legally compliant consent forms in which users get actively engaged with the content. Active engagement with the content of a consent form, using interaction techniques, for example, to select personal data to share, and for which permission for data processing is being sought by an IdP, can serve as an affirmative action: a clear indication of a user's willingness to accept the permission.

As our results show, the most efficient way of engaging users with the content may not necessarily be the most effective way and also the most satisfactory way for users. For example, using checkboxes to opt-in in consent forms which is more common than any other methods nowadays may not be the most effective way, based on our results, for users to catch their attention and make them aware of their data flow. Furthermore, the methods which are not beneficial for users in the context of consent forms affect service providers as well. To be legally compliant, according to the GDPR, service providers should be able to show that they achieved *informed* consent from users. If the engagement method is not effective to help users to be aware of their data flow and the conditions of consent, service providers cannot rely on the permissions they acquire, may face financial fines, and may lose their customers' trust.

However, new design solutions to actively engage users with the content, come with their own challenges. For example, as users are unfamiliar with experiencing the new types of involvement in consent forms they may require some guidance and help at the beginning. This raises the question of how newer solutions such as DAD and swiping are stable in their effectiveness over time, as users gradually become more familiar with using them in consent forms. Stable effectiveness remains a subject for the future work.

Although we tested different interaction techniques utilised for selecting personal information in the permission dialogues of an IdP, our results are valid for consent forms in other contexts where users are requested to

select the information they want to share or the action they would like to take with their data.

Limitations: Because of ethical considerations and problems of implementation, the participants were given a persona to role-play for the task. Hence, neither personal identifying information was captured from participants nor any personal information was shown in the permission dialogues. One could argue that this had an impact on the users' attention to data collected in permission dialogues as they may not have felt any risk, or danger, with respect to their information privacy. On the other hand, as we compare different interaction designs under the same conditions, the results pertaining to differences in speed, SUS and Recall values between design solutions are valid, even though only for the type of participants we involved in this study. A clear limitation of this study is that it is not representative for the whole population of users of identity providers on smartphones. However, as the existence of differences between our designs is now established in this study, one can venture to further elaborate on these designs and on other user groups.

Reflecting on our results in context: When we reflect on the overview summary of the results of related work presented in Table 1 in the context of our results, we can appreciate that this problem of engaging users is challenging for researchers. Table 1 gives an overview of the research in this area, and shows the particular focus of various research groups. It would be unfair to compare the results from these studies directly with each other because the experiments were not conducted using the same methods. However, this overview is interesting because it highlights the different approaches to solve the problem of engaging users' attention to specific contents using interaction techniques, and it motivated our study, as explained in Section 2. Note that some researchers, based on the results of their studies, conclude that a precise understanding and recalling of the attributes users share with a service provider using the permission dialogues of an IdP might not be significantly affected by the content of consent forms (Bauer et al. 2013; Egelman 2013; Karegar et al. 2018b). Bauer et al. (2013) demonstrated that participants precise understanding of the information sent is affected by their privacy concern level and by the fact that they have some preconceptions about the information that is going to be sent. In contrast, we demonstrate here that not being affected by the content of consent forms is due to a lack of attention; users typically have preconceptions and guess about what is shared. When attention is improved the effect of the specific content of consent forms on user understanding and recalling of information can be improved. This motivates us further to undertake more research on the interaction techniques of consent forms, in order to improve user attention and engagement. For further discussion on the implications of our study, see Section 7.

7. Conclusion and future work

Our study comparing swiping, DAD and checkbox design of permission dialogues demonstrates that checkboxes while speedy do not engage the user in the way that DAD and swiping capture their attention. This suggests that the development of interfaces that involve the users in actively selecting data for sharing should be further developed and tested. Users' satisfaction rates are positively impacted by these newer methods of giving consent. Clearly, different design patterns have a notable impact on their perceived usability.

As one might expect, younger adults are, in general, faster in completing authorisation tasks than mature adults (over 30). However, the fact that we are unable to demonstrate a relationship between the time for the task and participants' Recall rates prompts further investigation. For future work, it will be very interesting to investigate if spending more time on a design also means more attention to important items on the dialogues. In such studies, direct methods to measure attention must be used such as eye-tracking. However, presently this is very difficult because of the imprecision of the eye-trackers.

In this study, we focus on user attention and awareness to the personal information directly requested in the permission dialogues. However, for a consent to be informed there are more issues of which users should be aware, and that must be communicated to them. The purposes of data processing and conditions of consent, such as retention time and how to revoke consent, are examples of information that users should know before they decide on how to handle a request, according to Article 13 of the GDPR (The European Parliament and the Council of the European Union 2016). Will users pay attention to data processing and data use policies if we only involve them in dialogues to select data types to be shared?

Besides a user's familiarity with the entities involved, users' trust or lack of trust in both the IdP and the service provider may play a significant role in their understanding and perception of the information that is shared. For example, if a participant answers 'not sure' for each data type, it might indicate they do not trust the identity provider or they do not trust the website.

Issues of trust, perception, and attention impact on the usability of an interface, and the effective use of authorisation dialogues. Until we can find ways to differentiate between these phenomena when evaluating user

interfaces, the legal requirements of informed consent will be under the control of the service providers.

Notes

1. Attractors which prevent users from making a potentially dangerous choice by either slowing them down or make them perform an action.
2. https://www.axure.com.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This research has received funding from the European Unions Horizon 2020 Research and Innovation Programme [grant number 65345] for the CREDENTIAL project.

References

Albert, William, and Thomas Tullis. 2013. *Measuring the User Experience: Collecting, Analyzing, and Presenting Usability Metrics*. Burlington: Morgan Kaufmann.

Assale, Michela, Erica Barbero, and Federico Cabitza. 2019. "Digitizing the Informed Consent: The Challenges to Design for Practices." In *32nd International Symposium on IEEE Computer-Based Medical Systems (CBMS)*. Cordoba, Spain, pp. 609–615. IEEE

Bangor, Aaron, Philip Kortum, and James Miller. 2009. "Determining What Individual SUS Scores Mean: Adding an Adjective Rating Scale." *Journal of Usability Studies* 4 (3): 114–123.

Bauer, Lujo, 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 *Proceedings of the 2013 ACM Workshop on Digital Identity Management, DIM '13*, New York, NY, 25–36. ACM.

Bhagavatula, Rasekhar, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, and Marios Savvides. 2015. "Biometric Authentication on iphone and Android: Usability, Perceptions, and Influences on Adoption." Proc. USEC. Internet Society.

Bravo-Lillo, Cristian, Saranga Komanduri, Lorrie Faith Cranor, Robert W. Reeder, Manya Sleeper, Julie Downs, and Stuart Schechter. 2013. "Your Attention Please: Designing Security-decision UIs to Make Genuine Risks Harder to Ignore." In *Proceedings of the Ninth Symposium on Usable Privacy and Security, SOUPS '13*, New York, NY, 6:1–6:12. ACM.

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

Brustoloni, José Carlos, and Ricardo Villamarín-Salomón. 2007. "Improving Security Decisions with Polymorphic and Audited Dialogs." In *Proceedings of the 3rd Symposium on Usable Privacy and Security, SOUPS '07*, New York, NY, 76–85. ACM.

Choi, Ben C. F., Samuel N. Kirshner, and Yi Wu. 2016. "Swiping vs. Scrolling in Mobile Shopping Applications." In *HCI in Business, Government, and Organizations: eCommerce and Innovation*, edited by Fiona Fui-Hoon Nah and Chuan-Hoo Tan, 177–188. Cham: Springer.

Cooper, Alan, Robert Reimann, and David Cronin. 2007. *About Face 3: The Essentials of Interaction Design*. Indianapolis: John Wiley.

Dou, Xue, and S. Shyam Sundar. 2016. "Power of the Swipe: Why Mobile Websites Should Add Horizontal Swiping to Tapping, Clicking, and Scrolling Interaction Techniques." *International Journal of Human-Computer Interaction* 32 (4): 352–362.

Egelman, Serge. 2013. "My Profile is My Password, Verify Me!: The Privacy/Convenience Tradeoff of Facebook Connect." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2369–2378. ACM.

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)."

Gluck, Joshua, Florian Schaub, Amy Friedman, Hana Habib, Norman Sadeh, Lorrie Faith Cranor, and Yuvraj Agarwal. 2016. "How Short Is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices." In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, Denver, CO, 321–340. USENIX Association.

Hoekman Jr., Robert. 2010. *Designing the Obvious: A Common Sense Approach to Web & Mobile Application Design*. Berkeley: Pearson Education.

Hörandner, F., S. Krenn, A. Migliavacca, F. Thiemer, and B. Zwattendorfer. 2016. "CREDENTIAL: A Framework for Privacy-Preserving Cloud-Based Data Sharing." In *2016 11th International Conference on Availability, Reliability and Security (ARES)*, August, 742–749.

ISO. 2018. "9241-11:2018. Ergonomics of Human-System Interaction – Part 11: Usability: Definitions and concepts." International Standardization Organization (ISO).

Javed, Yousra, and Mohamed Shehab. 2016. "Investigating the Animation of Application Permission Dialogs: A Case Study of Facebook." In *International Workshop on Data Privacy Management (DPM)*, 146–162. Springer.

Javed, Yousra, and Mohamed Shehab. 2017. "Look Before You Authorize: Using Eye-Tracking to Enforce User Attention Towards Application Permissions." *Proceedings on Privacy Enhancing Technologies (PoPET)* 2 (2): 23–37.

Karegar, Farzaneh, Nina Gerber, Melanie Volkamer, and Simone Fischer-Hübner. 2018a. "Helping John to Make Informed Decisions on Using Social Login." In *Proceedings of the 33rd Annual ACM Symposium on Applied Computing, SAC '18*, New York, NY, 1165–1174. ACM.

Karegar, Farzaneh, Daniel Lindegren, John Sören Pettersson, and Simone Fischer-Hübner. 2018b. "User Evaluations of an App Interface for Cloud-Based Identity Management." In *Advances in Information Systems Development*, edited by Nearchos Paspallis, Marios Raspopoulos, Chris Barry, Michael Lang, Henry Linger, and Christoph Schneider, 205–223. Cham: Springer.

Karegar, Farzaneh, John Sören Pettersson, and Simone Fischer-Hübner. 2018. "Fingerprint Recognition on Mobile Devices: Widely Deployed, Rarely Understood." In *Proceedings of the 13th International Conference on Availability, Reliability and Security, ARES 2018*, New York, NY, 39:1–39:9. ACM.

Kobsa, Alfred, and Maximilian Teltzrow. 2005. "Contextualized Communication of Privacy Practices and Personalization Benefits: Impacts on Users' Data Sharing and Purchase Behavior." In *Privacy Enhancing Technologies*, edited by David Martin and Andrei Serjantov, 329–343. Berlin: Springer.

Kostopoulos, Alexandros, Evangelos Sfakianakis, Ioannis Chochliouros, John Sören Pettersson, Stephan Krenn, Welderufael Tesfay, Andrea Migliavacca, and Felix Hörandner. 2017. "Towards the Adoption of Secure Cloud Identity Services." In *Proceedings of the 12th International Conference on Availability, Reliability and Security, ARES '17*, New York, NY, 90:1–90:7. ACM.

Malhotra, Naresh K, 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): 336–355.

Morrison, Alistair, Donald McMillan, and Matthew Chalmers. 2014. "Improving Consent in Large Scale Mobile HCI through Personalised Representations of Data." In *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational, NordiCHI '14*, New York, NY, 471–480. ACM.

Murray, Janet H. 2011. *Inventing the Medium: Principles of Interaction Design as a Cultural Practice*. MIT Press.

Norman, Don. 2013. *The Design of Everyday Things: Revised and Expanded Edition*. New York: Constellation.

Patrick, Andrew S., and Steve Kenny. 2003. "From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interactions." In *Privacy Enhancing Technologies*, edited by Roger Dingledine, 107–124. Berlin: Springer.

Pettersson, John Sören, Simone Fischer-Hübner, Ninni Danielsson, Jenny Nilsson, Mike Bergmann, Sebastian Clauss, Thomas Kriegelstein, and Henry Krasemann. 2005. "Making PRIME Usable." In *Proceedings of the 2005 Symposium on Usable Privacy and Security (SOUPS)*, 53–64. ACM.

Ronen, Shahar, Oriana Riva, Maritza Johnson, and Donald Thompson. 2013. "Taking Data Exposure into Account: How Does It Affect the Choice of Sign-In Accounts?" In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 3423–3426. ACM.

Ruoti, Scott, Brent Roberts, and Kent Seamons. 2015. "Authentication Melee: A Usability Analysis of Seven Web Authentication Systems." In *Proceedings of the 24th International Conference on World Wide Web*, 916–926. International World Wide Web Conferences Steering Committee.

Ruoti, Scott, and Kent Seamons. 2016. "Standard Metrics and Scenarios for Usable Authentication." In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. Denver, CO: USENIX Association.

Sears, Andrew, Julie A. Jacko, and Erica M. Dubach. 2000. "International Aspects of World Wide Web Usability and the Role of High-End Graphical Enhancements." *International Journal of Human-Computer Interaction* 12 (2): 241–261.

Sindhuja, P. N., and Surajith Ghosh Dastidar. 2009. "Impact of the Factors Influencing Website Usability on User Satisfaction." *IUP Journal of Management Research* 8 (12): 54–66.

Sundar, S. Shyam. 2007. "Social Psychology of Interactivity in Human-Website Interaction." In *The Oxford handbook of Internet psychology*, edited by Adam N. Joinson, Katelyn Y. A. McKenna, Tom Postmes, Ulf-Dietrich Reips, and S. Shyam Sundar, 89–104. Oxford: Oxford University Press.

Sundar, S. Shyam, Saraswathi Bellur, Jeeyun Oh Qian Xu, and Haiyan Jia. 2014. "User Experience of On-Screen Interaction Techniques: An Experimental Investigation of Clicking, Sliding, Zooming, Hovering, Dragging, and Flipping." *Human-Computer Interaction* 29 (2): 109–152.

Tabassum, Madiha, Abdulmajeed Alqhatani, Marran Aldossari, and Heather Richter Lipford. 2018. "Increasing User Attention with a Comic-Based Policy." In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, CHI '18*, New York, NY, 200:1–200:6. ACM.

Vetenskapsrådet. 2002. *Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning*. Stockholm, Sweden: Vetenskapsrådet.

Wang, Na, Jens Grossklags, and Heng Xu. 2013. "An Online Experiment of Privacy Authorization Dialogues for Social Applications." In *Conference on Computer Supported Cooperative Work (CSCW)*, 261–272. ACM.