sciendo

Proceedings on Privacy Enhancing Technologies ; 2022 (1):629–648

Moses Namara*, Henry Sloan, and Bart P. Knijnenburg

The Effectiveness of Adaptation Methods in Improving User Engagement and Privacy Protection on Social Network Sites

Abstract: Research finds that the users of Social Networking Sites (SNSs) often fail to comprehensively engage with the plethora of available privacy features—arguably due to their sheer number and the fact that they are often hidden from sight. As different users are likely interested in engaging with different subsets of privacy features, an SNS could improve privacy management practices by adapting its interface in a way that proactively assists, guides, or prompts users to engage with the subset of privacy features they are most likely to benefit from. Whereas recent work presents algorithmic implementations of such privacy adaptation methods, this study investigates the optimal user interface mechanism to present such adaptations. In particular, we tested three proposed *"adaptation methods"* (automation, suggestions, highlights) in an online between-subjects user experiment in which 406 participants used a carefully controlled SNS prototype. We systematically evaluate the effect of these adaptation methods on participants' engagement with the privacy features, their tendency to set stricter settings (protection), and their subjective evaluation of the assigned adaptation method. We find that the *automation* of privacy features afforded users the most privacy protection, while giving privacy *suggestions* caused the highest level of engagement with the features and the highest subjective ratings (as long as awkward suggestions are avoided). We discuss the practical implications of these findings in the effectiveness of adaptations improving user awareness of, and engagement with, privacy features on social media.

Keywords: privacy, social media, Facebook, user-tailored privacy, privacy on social media, privacy decision-making

DOI 10.2478/popets-2022-0031
Received 2021-05-31; revised 2021-09-15; accepted 2021-09-16.

1 Introduction

Social networking sites (SNS) like Facebook play an essential role in people's social and personal lives. In particular, Facebook has become integral in the maintenance of social relationships, social interactions, self-representation, connectedness, entertainment, and professional activities [1]. The incorporation of all these functionalities and activities within the platform has blurred the boundaries between public and private sharing environments depending on the context of use [2, 3]. In an effort to enable users to set and manage their privacy boundaries, Facebook developed a plethora of privacy features that can be used to manage disclosure on the platform [2, 4]. However, users are unaware of most of these privacy features, report finding them confusing, and encounter difficulties in discovering and engaging them [5–8]. As a result, these privacy features remain underutilized despite efforts to improve users' awareness and subsequently engagement [8, 9].

Several researchers have investigated ways in which user awareness, engagement and utilization of privacy features can be improved [4, 10–15]. This paper specifically addresses *adaptive approaches* that involve modelling user privacy preferences and automatically tailoring privacy settings to match these preferences [10, 12, 14, 16]. Researchers assert that, by proactively striking a personalized balance between users' desire for privacy and their need for online interaction, such approaches could help users achieve the privacy they want without overwhelming them with privacy features [10].

Whereas ample existing work covers algorithmic approaches to privacy preference modeling [12–15, 17–19], relatively little research has examined the appropriate means through which personalized privacy adaptations can be presented to the user [16, 20, 21]. This work is important, since the optimal "adaptation method" can help users to meaningfully engage with the avail-

***Corresponding Author: Moses Namara:** Clemson University, E-mail: mosesn@clemson.edu
Henry Sloan: Binghamton University, E-mail: henryksloan@gmail.edu
Bart P. Knijnenburg: Clemson University, E-mail: bartk@clemson.edu

able privacy features without overwhelming or misleading them [16]. Increasing user engagement would help give users more active ownership over their privacy. In this light, Namara et al. proposed three *"adaptation methods"*—ways in which suggested behaviors (i.e., privacy adaptations) can be presented to the user[16] that vary in the level of autonomy and control they afford to users in the privacy decision making process [22]. Namely: 1) *automation* involves the automatic application of the privacy settings by the system without user input; 2) *highlights* emphasize certain privacy features to guide users to apply the settings themselves; and 3) *suggestions* explicitly inform users about the availability of certain settings that can then be applied directly by the user [16]. While a preliminary study has investigated users' initial perceptions towards the application of these adaptation methods [16, 20], it remains unclear how effective these adaptation methods would be at protecting user privacy.

Thus, in this study, we examine the effectiveness of the adaptation methods suggested by Namara et al. [16]—automation, highlights, and suggestions—in improving users' engagement with the available privacy features and their overall levels of privacy protection. Specifically, we answer the following questions:

RQ1: Which adaptation method(s) are effective at improving user engagement with the privacy features?

RQ2: Based on their default application and user engagement patterns, which adaptation method(s) offer better overall privacy protection outcomes?

RQ3: Which adaptation method(s) do users find most helpful?

The remainder of this paper is structured as follows: After a discussion of relevant related work in Section 2, Section 3 describes a between-subjects online user experiment in which 406 participants interacted with a carefully controlled working prototype of an SNS platform designed to look and feel like Facebook. This section describes the adaptation methods in more detail, and outlines how the study measured the effect of these adaptation methods on participants' engagement with the privacy features, their tendency to set stricter settings (for privacy protection), and their subjective evaluation of the assigned adaptation method.

Section 4 discusses our findings: 1) the automation of privacy settings affords users the most privacy protection without decreasing user engagement, 2) offering privacy suggestions increases engagement even further, and ultimately also enhances privacy protection (although not as much as automation), 3) users find privacy suggestions the most helpful, but only if the adaptation method avoids privacy features that could potentially result in awkward suggestions, and 4) highlighting privacy features neither increases users' engagement with the privacy features nor their privacy protection levels.

Section 5 discusses the results alongside previous research findings showing that users gain the most when social network sites give them the level of privacy they desire [10] and that users would prefer the suggestion method as means to teach them about privacy features they are unfamiliar with and ultimately improve their awareness and engagement with privacy features [16]. Finally, Sections 6 & 7 discuss the limitations of our work and future work respectively. Section 8 concludes the paper by summarizing how this study contributes to the privacy community's understanding of how users can be helped in the management, control and automatic setting of their desired level(s) of privacy.

2 Related Work

In the following subsections we first review the related work on SNS (e.g.,Facebook) users' privacy feature awareness, engagement, and the potential of a self-adaptive approach (e.g., user-tailored privacy) in helping users manage and safeguard their privacy. Subsequently, we review the related literature on Facebook users' common privacy behaviors and features.

2.1 Facebook Users' Privacy Feature Awareness and Engagement

Facebook users use the platform to communicate and socialize with friends and family, network and search for career opportunities, share thoughts, relevant news, feelings, emotions, news, stories, pictures and videos of various life events [23, 24]. To successfully support all these use cases, Facebook offers users a number of privacy features to control how they interact and share information with each other [25]. These privacy features are supposed to help users set their desired level of privacy in sufficient detail. However, user awareness of these privacy features remains low [4, 5], and most users end up not using the available privacy features [2, 4–6].

For instance, in their study on user awareness of News Feed controls on Facebook, Hsu et al.[5] found

that 49% of Facebook users were not aware of the existence of many of the features that they could use to personalize their feed. Even when users had the desire to use the existing controls, they struggled to find them. The authors also found that there was a misalignment between users' expectations and the actual functionality provided by the features [5]. Liu et al. [17] also found that available privacy features matched users' expectations only 37% of the time, and that incorrect expectations almost always meant that users underestimated the extent to which their information was exposed to others. As a result, they estimated that about 36% of all content on Facebook is posted with a privacy setting that shares it to more people than expected.

This lack of awareness and misalignment of privacy features has important ramifications for both new and experienced Facebook users [26]. Our work provides insights into the application of *adaptive support* to improve Facebook users' privacy management practices. In particular, we offer recommendations on how various adaptation methods can be used to increase user engagement with the available privacy features, and to reduce the mismatch between users' desired level of privacy protection and the system's actual privacy settings.

2.2 A Self-Adaptive Approach: User Tailored Privacy (UTP)

Several privacy scholars have advocated for user-tailored privacy (UTP) as a privacy-enhancing adaptive approach that can be used to improve users' awareness of, and engagement with, privacy features [12, 16, 27, 28].The idea behind UTP is to measure users' privacy preferences and behaviors, use these measurements to create a personalized model of the user's privacy preferences, and then provide adaptive support to the user in navigating the available privacy settings—or even automatically implement certain settings automatically on the user's behalf [12].

A growing body of research has focused on the development of personalized models that align with users' privacy preferences. For example, Liu et al.[17], analyzed privacy preferences and permission-granting behaviors of 4.8 million Android users. They found that although people's mobile app privacy preferences are diverse, a small number of profiles could actually be identified to simplify their privacy-decision making processes. Similarly, Wijesekera et al. [15] built a classifier that could make mobile app permission decisions on the user's behalf by detecting a change in their context, and when necessary, inferring user privacy preferences based on their past decisions and behaviors. The resultant classifier accurately predicted users' privacy decisions 96.8% of the time.

Studies in the context of location-sharing applications have also developed personalized models that align privacy settings with users' privacy preferences. For instance, Toch et al [29] found that people who tend to visit a wider variety of places tended to be subjected to a greater number of requests for their locations. However, users were only comfortable granting permission if the location was typically visited by a large and diverse set of people. Benisch et al [30] found that privacy-setting schemes were more accurate at capturing users' location sharing preferences if they were dependent on both time and location. Ravichandran et al [18] found that decision-tree and clustering algorithms could be used to provide users with a small number of basic default policies to choose from to alleviate the burden involved in sharing locations with location-based apps and abstract away user-specific elements (e.g., a user's default schedule or canonical places such as "work" and "home").

A series of studies in the broader context of the Internet of Things built similar user models clustering users' privacy decisions into a number of privacy profiles [13, 19, 31]. For instance, Bahirat et al. [13], developed a set of three "smart" default profiles that captured users' preferences towards sharing data with public IoT systems. He et al. [19] used a similar approach to predict users' smarthome privacy preferences with five profiles, and Sanchez et al. developed a four-tier profile-based system to predict users' privacy preferences in the context of wearable fitness trackers. In each case, the profile-based solution was able to capture users' preferences with an accuracy of around 82-85%.

In the context of social networks, Fang and LeFevre [32] used a similar profile-based approach in the development of a privacy wizard that automatically assigns privileges to a user's Facebook friends. The evaluation of the wizard with privacy preference data collected from 45 real Facebook users revealed that the it could generate highly accurate settings to automatically assign to a user's friends with minimal user input.

While this prior work has identified methods to create personalized models that can be used to adapt a system's privacy settings to the user's preferences, limited research has focused on the design and presentation of these adaptations [14, 16, 20, 21, 33]. Our work seeks to address this gap by examining the effectiveness of various adaptation methods that can be used to present privacy adaptations to users.

2.3 Presenting Privacy Adaptations

Limited research effort has been devoted to the exploration of the *presentation* of privacy adaptations that align with user privacy preferences. The concept of "presentation" goes beyond the visual characteristics of the adaptation and can have a profound impact on the required level of engagement with the system and the user's tendency to follow the suggested adaptation. For example, while some propose to fully automate the privacy decision-making process (e.g. [34]), others have implemented adaptive suggestions (e.g. [14], or suggested the use of personalized nudges (e.g. [28]) or interface adaptations (e.g. [21]).

Liu et al. [14] found that mobile app permission setting suggestions based on user privacy preferences were perceived to be helpful and largely adopted by users. Most importantly, the suggestions increased user engagement with the privacy settings.

Warberg et al. [28] reaffirmed the importance of examining the possibilities of tailoring privacy nudges to align with individual differences in decision making and personality, especially among large organizations such as SNS that typically have a large number of users.

Wilkinson et al. [21] recognized that the privacy features on social networks are often more than one click away, and explored the idea of adapting the social network User Interface (UI) in such a way that it increases the salience of those features that fit the user's personal privacy management strategy (cf. [4]).

While this existing work has explored different methods of adaptively assisting users with their privacy management practices, all but two papers (i.e. [16, 20]) have compared various adaptation method in terms of their effectiveness at enhancing user engagement and overall privacy protection. The first exception, Namara et al. [16], identified three adaptation methods—Automation, Highlight, and Suggestions—that varied in the level of autonomy and control afforded to users (ranging from full control to no control [22, 35]) in managing their privacy. The authors created mockup screenshots of each of the three adaptation methods for 19 of the privacy features catalogued by Wisniewski et al. [4] (see Section 2.4). They found that the preferred adaptation method depended on the user's familiarity with the privacy feature, their past usage of the feature, and their judgement on whether the feature was or would be awkward to adapt or could result in irreversible negative consequences once adapted [16].

The second exception, Colnago et al. [20], adopted the adaptation methods used by Namara et al. in the design of different automation levels for a personalized Internet of Things (IOT) privacy assistant (PPA). They found that in choosing an appropriate adaptation method, users weigh their desire for control against their fear of cognitive overload in making privacy decisions.

Inspired by both Namara et al. [16] and Colnago et al. [20], our current work implements the same three adaptation methods in a functional but carefully controlled SNS UI prototype. Whereas Namara et al. and Colnago et al. used an interview-based approach to elicit users' evaluations of the three adaptation methods using UI screenshots/descriptions, our study primarily aimed to test users' privacy management behaviors in the context of a controlled but semi-realistic SNS environment implementing one of the adaptation methods. This approach allowed us to gain an empirical understanding of the effectiveness of the adaptation method in improving user engagement and their overall level of privacy protection.

Although the three adaptation methods have been described in Namara et al. and Colnago et al., we reiterate their definitions below, adding the attitudinal findings of Namara et al. [16] and Colnago et al. [20] where appropriate. Note that the depicted mockups are screenshots from our study.

Automation: The "Automation" adaptation method involves the automatic manipulation of a privacy feature without first requesting user permission. While this adaptation method can operate completely outside of the user's awareness, our implementation does leave a message on the privacy feature informing the user of the automated action taken by the system on their behalf. For example, when a user is automatically untagged from a post, the tag would be removed and replaced with a message informing them that they were automatically untagged (see Fig. 1). Coupled with the message is a small "*Undo*" button that allows the user to reverse the automated action if they are uncomfortable with the automated setting.

Namara et al. [16] found that the Automation adaptation method was generally disliked, except for privacy features that were used frequently and perceived as inconsequential (i.e., automation application of the privacy feature would not result into real-world negative consequences such as loss of real-world friendships due to automatic unfriendship or blockage on social media). In this case, automation could help alleviate the cognitive burden involved in privacy management. Colnago et al. [20] also found that users were split about the Automation adaptation method. In their context, a third of participants disliked the idea out of concern of the PPA

making poor decisions for them, while two-thirds of the participants had a positive opinion as long as automation could help remind and encourage them to continue doing something they had done well in the past. The other third of the participants were also comfortable with automation based on the premise that it reduced the cognitive burden related to privacy decision-making. However, the trust users had in the automated decision was likely to be influenced by the justification for automation, trust and experience with other predictive technologies from the PPA company.

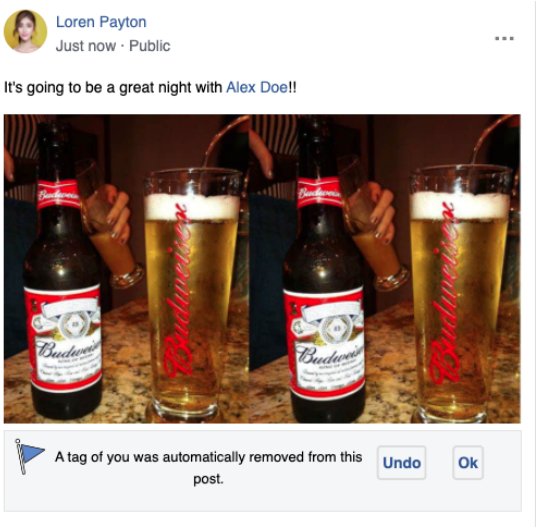

Fig. 1. The automation adaptation of the privacy feature for *"untagging oneself from a post"* in our SNS UI mockup

Highlight: The "Highlight" adaptation method involves increasing the visual prominence of a privacy feature—a subtle "nudge" that is meant to encourage the user to undertake a certain privacy action. This is achieved by highlighting the background of the privacy feature using a highly contrasting color (in our study: a yellow background color). Note that our SNS UI mockup is based on the Facebook UI, in which many privacy features are hidden behind menu options or have multiple navigation pathways. The highlight implementation therefore illuminates not only the privacy feature itself, but also the path towards it. For example, when a user is tagged in a post, the Highlight adaptation to untag the user emphasizes both the context menu button that contains the "Remove tag" feature as well as the feature itself (see Fig 2).

Namara et al. [16] found that the Highlight adaptation method was appreciated by users for its ability to unobtrusively raise users' awareness about a privacy feature. Colnago et al. [20] found that the Highlight adaptation method (conceptualized as a "notification" in the context of their study) was liked by users since it helped raise their awareness about the presence of nearby IOT devices that requested their personal information.

Fig. 2. The highlight adaptation of the privacy feature for *"untagging oneself from a post"* in our SNS UI mockup

Suggestions: The "Suggestion" adaptation method involves proactively recommending the privacy action to the user. Namara et al. [16] display the recommendation message using a virtual character ("agent") to increase its prominence and to be more endearing [36]. Moreover, although recommendation messages can vary in tone and framing, Namara et al. use a positive framing (i.e. nudge the user towards taking the suggested action), giving the user the option to accept ("*Ok*") or reject ("*Rather Not*") the recommended action. We use the same implementation as Namara et al. [16] (see Fig 3) because their particular implementation was well-received in their interview study. We leave the investigation of alternative versions of this adaptation method for future work. If users click "*Ok*" the suggestion is implemented directly. If the suggestion appears in places where the privacy feature is not directly on the user's screen, users are transferred to the page or point where the feature appears, so that they can verify the adaptation and adjust the setting if needed.

Namara et al. [16] found that the Suggestion adaptation method was preferred as a means of teaching users privacy features that they were unfamiliar with, unless the the feature was awkward to suggest or had a negative social connotation (i.e., whose suggestion would break certain social norms with regards to private behaviors that carry a negative social perception

e.g., deleting posts and unfollowing users). Similarly, Colnago et al. [20] found that the Suggestion adaptation method (conceptualized as a "recommendation" in the context of their study) was preferred as an educational tool.

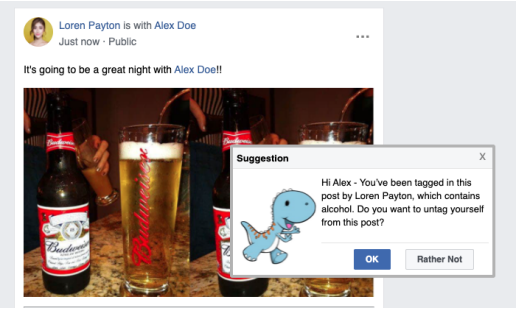

Fig. 3. The suggestion adaptation of the privacy feature for *"untagging oneself from a post"* in our SNS UI mockup

While our adaptation methods are directly based on Namara et al. [16] (and indirectly on Colnago et al. [20]), we iterate here that our work expands on these two works in four significant ways: 1) by using a working prototype of an SNS in an experiment instead of adaptation descriptions or low-fi prototypes, we are able to obtain an empirical understanding of users' engagement behaviors when presented with actual privacy adaptations of social media privacy features using the proposed adaptation methods (see Appendix D, Table 3 for a list of the adapted privacy features); 2) beyond the three proposed adaptation methods, we test a few subtle variants (differentiated using the label "some" within the setup of the experimental conditions) which forego the automation of certain privacy features that have seemingly irreversible consequences (e.g., blocking a person, blocking app invites, blocking event invites) [16, 25], avoid awkward suggestions (e.g., blocking a person, blocking app invites, blocking event invites, deleting a post) [16, 25], and/or tailor the adaptation method of each privacy feature to the user's awareness of and previous experience with the feature; 3) beyond users' subjective evaluations of the adaptation methods, we examine the effects of the adaptation methods on the level of user engagement and on the overall level of privacy protection; and 4) beyond qualitative findings, we provide a quantitative evaluation of what adaptation method(s) participants found most helpful.

2.4 Facebook Users' Privacy Behaviors and Features

Wisniewski et al. [2] identified and categorized an exhaustive set of prevalent boundary regulation mechanisms supported on social media platforms. They found that Facebook supported its users' privacy preferences through features that facilitated management of access to oneself (e.g., blocking other users, or hiding one's online status to avoid unwanted chats), management of personal information (e.g., withholding contact or basic info), management of interpersonal interactions (e.g., friending and unfriending), management of virtual spaces (untagging posts or photos or deleting unwanted content posted by others), and management of interactions between networks (e.g., hiding one's friend list from others). In a follow up study, the authors identified 36 privacy features users often used to perform these privacy behaviors [4]. They analyzed the behavioral patterns in a collected dataset and found that the users' engagement with the identified features loaded onto 11 distinct latent factors. Moreover, they were able to identify 6 groups of participants who employed distinctly different privacy management strategies to achieve their desired level of privacy. Namara et al. adopted 19 of the privacy features identified by Wisniewski et al. [4], making sure to include features from all 11 identified factors. To make our study more manageable, we further reduced the number of privacy features to 13, still keeping at least one from each of the 11 identified factors.

3 Methods

Our user experiment aimed to examine the effectiveness of adaptation methods—automation, highlights, and suggestions, specifically adapted from Namara et al [16]—in improving user engagement and overall privacy protection.

Going beyond previous work [16, 20], we specifically examined the actions users took when privacy features were adapted and presented using these adaptation methods. The Clemson University Institutional Review Board (IRB) approved our study.

3.1 The SNS User Interface Mockup

Participants interacted with a carefully controlled working prototype of an SNS platform ("*FriendBook*", see Appendix C, Fig. 7). To increase the realism and ecological validity of the experiment, the FriendBook UI was based on the UI of the Facebook web application[1] and populated with posts using the Tweet corpus collected by Cachola et al. [37]. Each user saw the exact same posts, friends, etc., thereby guaranteeing that all users had the same opportunities to engage with the various privacy features. Using FriendBook allowed us to manipulate how we applied the adaptation methods to the adapted privacy features; in some conditions we applied the same adaptation method to all features, while in other conditions we avoided adapting certain features and/or or tailored the adaptation method to the user's awareness and past usage of each privacy feature (see Appendix E, Table 4, and Section 3.4 for a description of the experimental conditions).

As outlined in Section 2.4, we implemented adaptive versions of 13 privacy features (see Appendix D,Table 3 for descriptions) inspired by Wisniewski et al.'s [4] inventory of Facebook's privacy features. The selected 13 privacy features cover privacy behaviors commonly performed on Facebook such as altering the News Feed, managing profile information, friend management, limiting access control, blocking people/apps/events, restricting chat, and friend management [4]. The privacy features were similar in design and functionality to those found on Facebook.

All user interactions with the privacy features (adapted or not) were recorded and used to assess overall engagement patterns and privacy protection outcomes (see Section 3.5).

3.2 Study Setup

Participants were recruited between December 2019 and January 2020 via Amazon Mechanical Turk,a participant recruitment platform where people complete short tasks and receive automatic payments [38]. A total of 575 adult participants who were users of social media sites (e.g., Facebook) were recruited. We restricted participation to people within the United States with a high "worker reputation" (i.e., those with a HIT approval rate greater than 95% with at least 50 approved past HITs) to ensure satisfactory response quality. We also included several attention check questions and quality checks to remove participants who spent little time (less than 1 minute) within the study environment or who did not carefully read/respond to the pre- and post-survey questions [39]. After discarding 169 participants who did not meet our participation requirements and data quality checks, the valid data used in the analysis was from 406 [2] participants: (215 Men, 189 Women), aged between 18 and 60 (median category: 25-30).

3.3 Study Procedure

After reading the consent form and agreeing to partake in the study, participants completed a pre-survey. This pre-survey asked participants to indicate their awareness and past usage of each of the 13 privacy features (on Facebook). This was done by showing the participant an image of the privacy feature under examination and asking them 1) "Are you familiar with this Facebook feature: [Name of Feature]?" (response options: Yes, No) and 2) "How often do you use this feature?" (response options: Never Used, Used Once, Occasionally Use, Frequently Use). The responses to these questions enabled us to appropriately tailor the adaptation methods of each privacy feature based on their awareness and past use of the feature for the participants in experimental conditions C5 and C8 (see Section 3.4 for details on how the adaptation method was tailored in these conditions). Note that while this tailoring procedure was only implemented in conditions C5 and C8, all participants filled out the pre-survey to prevent this procedure from becoming a confounding variable.

A job search scenario was used as a motivating context in which participants could explore and manipulate the FriendBook profile used in the study. Specifically, participants were invited to imagine that:

> "*You are Alex Doe from Fresno, California and regularly use FriendBook (a social media site) for professional and leisure activities. You are currently looking for a job and have been advised by your mentor that employers monitor and scrutinize applicants' FriendBook profile before making decisions on whether to hire them or not. They have provided you with the following smart practices to consider*

1 FriendBook was developed before a new Facebook UI design was deployed in September 2020.

2 A power analysis, with α=.05, power=.97, df=7, and eight groups found that the suggested sample size (N=400) of a factorial ANOVA test was sufficient for detecting a medium effect (f=0.25)

about your profile as you go through the application process."

A list of smart practices (See example in Appendix A, Fig 6) was shown to participants following the scenario to ensure that they were cognizant of the types of tasks they could perform while on FriendBook. They were quizzed on this list to make sure that they paid attention to it. Together, the scenario and the list of smart practices helped participants navigate, engage, explore and review "their" profile on FriendBook. For easy recollection of the use context, the list of smart practices was also presented as a persistent sidebar throughout the user interaction process with FriendBook. (see Appendix C, Fig. 7). This list was carefully pilot-tested with the study target sample population (N = 25) to make sure that participants were properly motivated to manage their profile without explicitly demanding that they would engage in specific privacy management practices. Responses in our pilot-test debriefing interviews convinced us that participants would interact with the privacy features that *they themselves* thought to be the most appropriate ones to engage with.

Participants were subsequently asked to explore and interact with their profile on FriendBook, with the goal of ensuring that they were okay with what is on it, given the imagined upcoming job interview. In this phase, participants explored the various posts/friend, profiles/settings and—where appropriate—made changes using the available privacy features[3]. Depending on the experimental condition, (a subset of) the 13 privacy features would be adapted to the user using the designated adaptation method(s).

Upon completing the FriendBook task, participants were asked to evaluate the overall usefulness of the FriendBook platform (based on a scale adopted from [40]) and the perceived level of decision help they believed the platform provided (based on a scale adopted from [41]). Each participant was compensated with $3 for participating in the study.

3.4 Experimental Conditions

We developed a total of eight experimental conditions, with each condition applying the adaptation methods to the privacy features in a unique manner (see Appendix E ,Table 4 for an overview). Condition C1 served as a baseline where no adaptations were applied at all. In conditions C2-C4, all 13 privacy features were adapted to the user, using one of the three adaptation methods (Automation, Highlight, Suggestions, resp.).

Condition C5 was motivated by the results of Namara et al. [16], who concluded that it likely would be expedient to tailor the adaptation method itself to the user's prior knowledge and usage of the feature. Hence, in this condition the application of one of the adaptation methods was conditional upon participants' answers in the pre-survey regarding their familiarity with and usage of the privacy features (on Facebook): the Automation adaptation was applied to any privacy features the participant used frequently on Facebook; the Highlight adaptation was applied to any privacy features the participant used only occasionally; no adaptation was applied if the user had consciously decided not to use the privacy feature (i.e., they were aware of the privacy feature, but never used it or used it only once and then abandoned it); and the Suggestion adaptation was applied if the user was not aware of the adaptation (see Table 1 for an overview).

Condition C6 constituted a variant of condition C2, where the Automation adaptation method was applied to all privacy features *except* those features whose effect participants in Namara et al.'s study had deemed "irreversible", i.e., the three Block features (see Appendix D,Table 3). Similarly, Condition C7 constituted a variant of C4, where the Suggestion adaptation method was applied to all privacy features *except* those features for which participants in Namara et al.'s study had indicated that a suggestion would be "awkward", i.e., the three Block features, Unsubscribe from a friend, and Delete Post. Finally, condition C8 constituted a variant of condition C5, where the adaptation method of the privacy feature was tailored to the user, but where the Automation adaptation was avoided for "irreversible" features and the suggestion adaptation was avoided for "awkward" features (in those cases, no adaptation was applied).

3.5 Measurement

We recorded all user interactions with the privacy features to measure their engagement:

Manual accept: The participant "manually" interacted with a privacy feature that was not adapted,

3 Participants who spent too little time (<1 minute) interacting with FriendBook were removed from the analysis. The remaining participants spent an average of 5 minutes and minimum of 2 minutes on FriendBook.

Aware of privacy feature?	Usage of privacy feature	Adaptation Method
No	N/A	Suggestion
Yes	Never Used/Used Once	Default
	Occasionally Use	Highlight
	Frequently Use	Automation

Table 1. Adaptation method selection rules for the Tailor conditions (C5 & C8) as suggested by Namara et al. [16]

or they rejected the adaptation initially but then manually restricted their privacy after all.

Explicit accept: The participant explicitly accepted the adaptation, either by approving the suggestion (by clicking "Ok"), engaging with the highlighted feature, or verifying the automated adaptation (by clicking "Ok").

Implicit accept: The participant ignored an automated adaptation, thereby implicitly accepting it.

Implicit reject: The ignored highlighted feature or the suggested adaptation, or simply did not interact with the privacy feature at all.

Explicit reject: The participant explicitly rejected the suggestion (by clicking "Rather Not") or the automated adaptation (by clicking "Undo").

Based on these user actions, we assessed the overall engagement patterns (Section 4.1) and subsequently the privacy protection outcomes (Section 4.2) across all the eight experimental conditions. We define **positive engagement** as the adoption of the privacy feature adaptations accessed based on the sum of participants' manual engagement with the privacy features and their explicit acceptance of adaptations, and **negative engagement** as the explicit rejection of adaptations. We define **privacy protection** as the adoption of the privacy feature adaptations accessed based on the sum of participants' manual engagement with the privacy features, their explicit acceptance of adaptations, and their implicit acceptance of adaptations. For these three metrics, we used multilevel logistic regressions with a random intercept for participant to compare the odds of engagement / protection between the eight experimental conditions.

More specifically, we compared each adaptation condition (C2-C8) against the none condition (C1), compared between the adaptation conditions (C2-C5 for "all" and C6-C8 for "some"), and compared between the indiscriminate ("all") and selective ("some") variants of Automation (C2 vs. C6), Suggestions (C4 vs. C7) and Tailor (C5 vs. C8). Since we made a total of 19 comparisons per outcome variable, we corrected for familywise error using the Benjamini-Hochberg method[4] [42].

The post-study questionnaires assessing **perceived decision help** and the **perceived usefulness** of the platform were submitted to a confirmatory factor analysis. Both factors had a good reliability and convergent and discriminant validity [5]. Table 2, Appendix B shows the factor loadings, as well as Cronbach's alpha and average variance extracted (AVE) for each factor.

4 Results

Figure 4 shows the distribution of user actions in the eight experimental condition (C1-C8). Below, we first analyze the significant differences in **user engagement** between conditions, followed by the differences in **privacy protection**. We end this section with an analysis of users subjective evaluations (**perceived decision help** and **perceived usefulness**) between conditions.

4.1 Engagement Patterns

Figure 4 shows that participants rarely explicitly rejected an adaptation (by clicking "Rather Not" in a suggestion or by undoing an automated adaptation)—the prevalence of such **negative user engagement** in the conditions where it applied was only around 2%, and there were no statistical differences in negative engagement between these conditions ($\chi^2(5) = 10.756$, $p = .0564$). In the remainder of this subsection we analyze the differences in positive engagement only, and we will refer to it simply as "engagement".

We find that there are significant differences in **positive user engagement** (i.e., the sum of *manual accept* and *explicit accept*) across the eight experimental conditions ($\chi^2(7) = 97.987$, $p < .001$). We divide our exploration of the differences in positive user engagement into four subsections: In subsection 4.1.1 we compare

4 A post-hoc method that reduces α to account for family-wise error "by sequentially comparing the observed p-value for each of a family of multiple test statistics, in order from largest to smallest, to a list of computed B-H critical values" [42, p.78].

5 Cronbach's alphas > 0.8 indicate good reliability. AVEs > 0.5 indicate convergent validity, and $\sqrt{AVEs}$ higher than the inter-factor correlation indicate discriminant validity.

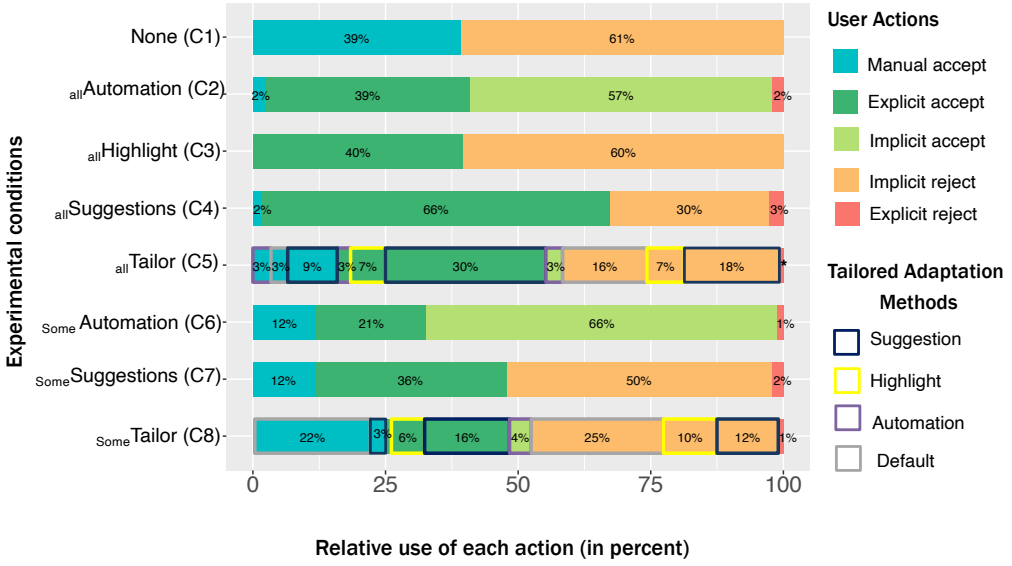

Fig. 4. Actions taken by participants across the eight experimental conditions. The level of positive user engagement is assessed by proportion of actions that are either manual or explicit accept, while the level of privacy protection is assessed by the proportion of actions that are either manual accept, explicit accept, or implicit accept ($*$ represents action counts $< 1\%$).

the levels of engagement in each adaptation condition (C2-C8) against the condition where no adaptions were applied (C1). We subsequently compare the levels of engagement among the conditions where all features were adapted (C2-C5, subsection 4.1.2) and among the conditions where awkward/irreversible features were avoided (C6-C8, subsection 4.1.3). We then compare the pairwise differences between the indiscriminate ("all") and selective ("some") versions of Automation, Suggestions, and Tailor in subsection 4.1.4, and conclude with a summary of the findings in subsection 4.1.5.

4.1.1 Suggestions and Tailored Adaptations Increase Engagement

On average, participants who interacted with the prototype that did not make any adaptations (C1) positively engaged with 39% of the privacy features. Comparing the level of engagement in all other conditions against C1, (positive) engagement is significantly higher for participants in the $_{all}$Suggestions (C4, 68%, $\beta = 1.30$, $p < .001$), $_{all}$Tailor (C5, 55%, $\beta = 0.70$, $p < .001$), $_{some}$Suggestions (C7, 48%, $\beta = 0.36$, $p < .001$), and $_{some}$Tailor (C8, 47%, $\beta = 0.39$, $p < .001$) conditions. Using the logistic regression βs to calculate odds ratios[6] ($e^{\beta} = OR$), we find that the odds of engaging with the privacy features are 3.67 times higher for participants in the $_{all}$Suggestions condition, 2.01 times higher for participants in the $_{all}$Tailor condition, 1.43 times higher for participants in the $_{some}$Suggestions condition, and 1.48 times higher for participants in the $_{some}$Tailor condition. These are small to medium-sized effects.

The differences in engagement between the None condition and the $_{all}$Automation (C2, 41%, $p = 0.291$), $_{all}$Highlight (C3, 40%, $p = 0.916$), and $_{some}$Automation (C6, 33%, $p = 0.94$) conditions are not significant.

These findings indicate that the level of user engagement with the available privacy features can be increased by providing privacy suggestions or by tailoring the adaptation method of the features to users' prior awareness and usage.

4.1.2 Among the "All" Conditions, Suggestions Lead to the Highest Engagement, Followed by Tailor

In this subsection, we present pairwise comparisons of the level of engagement among the adaptation con-

6 In the remainder of the paper we skip the β-coefficients and directly report the odds ratios. Odds ratios translate to effect sizes, with the values 1.68, 3.47 and 6.71 translating to small, medium and large effects.

ditions where *all* privacy features were adapted (i.e., $_{all}$Automation (C2), $_{all}$Highlight (C3), $_{all}$Suggestions (C4), $_{all}$Tailor (C5)).

On average, participants in the $_{all}$Suggestions condition positively engaged with 68% of the privacy features. Their odds of engaging with the features are 3.56 times higher than in the $_{all}$Automation condition (41%, $p < .001$), 3.77 times higher than in the $_{all}$Highlight condition (40%, $p < .001$), and 1.82 times higher than in the $_{all}$Tailor condition (55%, $p < .001$). Moreover, for participants in the $_{all}$Tailor condition, the odds of engaging with the features are 1.92 times higher than in the $_{all}$Automation condition ($p < .001$) and 2.03 times higher than in the $_{all}$Highlight condition ($p < .001$). The difference in engagement between the $_{all}$Automation and $_{all}$Highlight conditions is not significant ($p = .916$).

These findings indicate that the $_{all}$Suggestions adaptation resulted in a significantly higher level of engagement than any of the other conditions in which all privacy features were adapted, with the $_{all}$Tailor condition taking second place with a significantly higher level of engagement than the remaining two conditions.

4.1.3 Among the "Some" Conditions, Suggestions and Tailor Lead to the Highest Engagement

Namara et al. [16] recommended avoidance of the Suggestion adaptation for features that would be awkward to suggest or the Automation adaptation for features that would lead to seemingly irreversible consequences if automated. In this section, we present pairwise comparisons of the level of engagement among the adaptation conditions that avoided making such awkward/irreversible adaptations (i.e, $_{some}$Automation (C6), $_{some}$Suggestions (C7), $_{some}$Tailor(C8)).

Engagement is significantly higher in the $_{some}$Suggestions (48%) and $_{some}$Tailor (47%) conditions than in the $_{some}$Automation (33%) condition (see Fig 4). The odds of participants in the $_{some}$Suggestions condition in engaging with a privacy feature are 1.89 times higher than in $_{some}$Automation ($p < .001$) and the odds of participants in the $_{some}$Tailor condition ($p < .001$) engaging with a privacy feature are 1.99 times higher than in the $_{some}$Automation condition ($p < .001$). The difference between the $_{some}$Suggestions and $_{some}$Tailor conditions is not significant ($p = .913$).

These findings indicate that if awkward/irreversible adaptations are avoided, Suggestions and Tailoring both significantly increase engagement over Automation.

4.1.4 The "All" Conditions Generally Lead to Higher Levels of Engagement

In this subsection, we present pairwise comparisons of the level of engagement between the indiscriminate ("all") and selective ("some") versions of the Automation, Suggestions, and Tailor conditions (i.e., $_{all}$Suggestion(C4) Vs $_{some}$Suggestion (C7), $_{all}$Automation (C2) Vs. $_{some}$Automation (C6), and $_{all}$Tailor (C5) Vs $_{some}$Tailor (C8)).

The odds of engagement with the privacy features are 2.46 times higher in the $_{all}$Suggestions condition (68%) than in the $_{some}$Suggestions condition (48%, $p < .001$). Likewise, the odds of engagement are 1.52 times higher in the $_{all}$Automation condition (41%) than in the $_{some}$Automation condition (33%, $p < .001$). There is however no significant difference between the $_{all}$Tailor (55%) and $_{some}$Tailor (47%, $p = .0584$) conditions.

These findings indicate that the "all" conditions generally lead to higher levels of engagement than the "some" conditions—the awkward/irreversible adaptations did not discourage participants from positively engaging with the privacy features.

4.1.5 Summary of Engagement Findings

To summarize the findings regarding engagement:

- At 68%, the $_{all}$Suggestions condition leads to the highest levels of engagement—higher than the other "all" conditions and its "some" variant.
- The $_{all}$Tailor (55%), $_{some}$Tailor (47%), and $_{some}$Suggestions (48%) conditions also increase engagement compared to no adaptations—these are not significantly different from one another.
- Given that the Automation adaptation operates completely outside of the user's awareness, we are not surprised that the $_{all}$Automation and $_{some}$Automation conditions do not increase engagement compared to no adaptations (39%)—$_{all}$Automation (41%) leads to significantly higher engagement than $_{some}$Automation (33%), though.
- Surprisingly, Highlight (40%) did not increase engagement either, despite the visual prominence of the adaptations in this condition.

4.2 Privacy Protection Outcomes

While positive user engagement results in higher levels of privacy protection, some of the experimental condi-

tions (e.g., the Automation conditions) result in protection even when the user ignores the privacy features. In this subsection we analyze the differences in the average amounts of privacy protection participants end up with in each of the eight experimental conditions.

We find that there are indeed significant differences in the amounts of **privacy protection** (i.e., the sum of *manual accept*, *explicit accept*, and *implicit accept*) achieved across the eight experimental conditions ($\chi^2(7) = 391.45$, $p < .001$). We divide our exploration of these differences similarly to the engagement section: In subsection 4.2.1 we compare the level of privacy protection achieved in each adaptation condition (C2-C8) against the condition where no adaptions were applied (C1). We subsequently compare the level of privacy protection achieved in the conditions where all features were adapted (C2-C5, subsection 4.2.2) and among the conditions where awkward/irreversible features were avoided (C6-C8, subsection 4.2.3). We then compare the pairwise differences between the indiscriminate ("all") and selective ("some") versions of Automation, Suggestions, and Tailor in subsection 4.2.4, and conclude with a summary of the findings in section 4.2.5.

4.2.1 Apart From Highlight, All Adaptation Methods Improve Privacy Protection

In the prototype without adaptations (C1) participants are only protected if they engage with a feature. Hence, their protection is equal to their level of engagement: 39%. In contrast, protection is enabled-by-default in the $_{all}$Automation condition (C2), unless the user intervenes through an *explicit reject* action. Such actions are rare, hence the privacy protection in the $_{all}$Automation condition is virtually perfect, at 98%. Notably, although some of the privacy features are not adapted in $_{some}$Automation condition (C6), users seem to manually engage with those privacy features anyway, leading to virtually perfect privacy protection (99%) in this condition as well. Unsurprisingly, the pairwise differences between these conditions and the None condition are strongly significant ($p < .001$).

Further comparisons with C1 reveal that the odds for achieving privacy protections are 3.67 times higher for participants in the $_{all}$Suggestions condition (C4, 68%, $p < .001$), 2.01 times higher for participants in the $_{all}$Tailor condition (C5, 58%, $p < .001$), 1.42 times higher for participants in the $_{some}$Suggestions condition (C7, 48%, $p < .001$), and 1.48 times higher for participants in the $_{some}$Tailor condition (C8, 51%, $p < .001$). The privacy protection outcomes for the participants in $_{all}$Highlight condition (C3, 40%) are not significantly different ($p = 0.916$).

These findings indicate that all adaptation methods lead to better privacy protection outcomes, except for the Highlight adaptation.

4.2.2 A Clear Privacy Protection Hierarchy Exists Among the "All" Conditions

In this subsection, we present pairwise comparisons of privacy protection outcomes among the adaptation conditions where *all* privacy features were adapted.

As mentioned before, the protection in the $_{all}$Automation condition (98%) is virtually perfect—strongly significantly higher than all other "all"conditions. Among the remaining "all" conditions, the protection odds in the $_{all}$Suggestions condition (68%) are 3.78 times higher than in the $_{all}$Highlight condition (40%, $p < .001$) and 1.82 times higher than in the $_{all}$Tailor condition (58%, $p < .001$). Moreover, the protection odds in the $_{all}$Tailor condition are 2.03 times higher than in the $_{all}$Highlight condition ($p < .001$).

These findings show a clear hierarchy in privacy protection, with $_{all}$Automation providing the highest level of protection, followed by $_{all}$Suggestions, then $_{all}$Tailor, and finally $_{all}$Highlight.

4.2.3 Among the "Some" Conditions, Automation Leads to the Highest Level of Protection

In this subsection, we present pairwise comparisons of privacy protection outcomes among the adaptation conditions that avoided making awkward/irreversible adaptations. The privacy protection outcomes in the $_{some}$Automation condition (99%) is virtually perfect and hence strongly significantly higher than the $_{some}$Suggestion (48%) and $_{some}$Tailor (51%) conditions. The privacy protection odds between the latter two did not differ significantly ($p = .913$).

These findings indicate that even when features that are awkward/irreversible to adapt are avoided, automation still affords the best privacy protection outcomes.

4.2.4 Some Differences Exist Between the "Some" and "All" Conditions

Pairwise comparisons between the indiscriminate ("all") and selective ("some") conditions reveal that the privacy protection odds are 2.47 times higher in the $_{all}$Suggestion condition (68%) than the $_{some}$Suggestion condition (48%, $p < .001$). This result mirrors the engagement results, as the Suggestion conditions do not contain an "implicit accept" option.

The privacy protection odds are 1.87 times higher in the $_{some}$Automation condition (99%) than in the $_{all}$Automation condition (98%, $p < .001$). This is is surprising: even though the $_{some}$Automation foregoes automating certain features, the overall level of protection is higher than in the $_{all}$Automation, arguably because explicit rejections are lower in the former condition and because participants manually engage with the features that were not adapted.

Finally, there was no significant difference in privacy protection between the $_{all}$Tailor (58%) and $_{some}$Tailor (51%) conditions ($p = .0584$).

4.2.5 Summary of Privacy Protection Findings

To summarize the findings regarding privacy protection:

- At 98% and 99% respectively, the $_{all}$Automation and $_{some}$Automation clearly lead to the highest levels of privacy protection—this is evident by the relatively low incidence of explicit rejections.
- The fact that $_{some}$Automation outperforms $_{all}$Automation in terms of privacy protection speaks to the apparent superiority of this more prudent approach. Users seem to implement the avoided adaptations anyway, while at the same time issuing fewer explicit rejections.
- The $_{all}$Suggestions condition (68%) follows in third place, with a higher level of protection than $_{all}$Tailor (58%) and $_{some}$Tailor (51%) as well as $_{some}$Suggestions (48%).
- The $_{all}$Highlight condition (40%) performs worst, offering no significant protection benefits over no adaptations at all (39%).

4.3 Subjective Evaluations

In the assessment of the user subjective evaluations of the platform, we find that the **perceived decision help** and **perceived usefulness** measurement scales were highly correlated ($r = 0.858$). For the sake of completeness we include results from both scales (see Fig. 5). Compared to the condition where no adaptations were applied (C1), participants in the $_{some}$Suggestion condition (C7) deemed the platform more helpful ($\beta = 0.677$, $p < .001$) and more useful ($\beta = 0.677$, $p < .001$). While all other adaptation conditions were also deemed more helpful and useful than C1, none of these differences were significant.

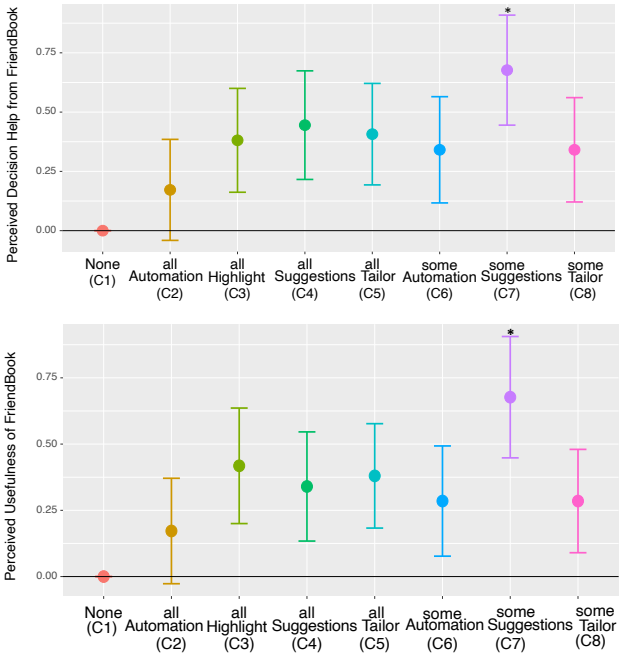

Fig. 5. The effect of the experimental conditions on perceived decision help and perceived usefulness. Factors have no inherent scale, so their values are fixed to zero for C1, and scaled in sample standard deviations of the measured factor. Error bars are ±1 standard error of the comparison with C1. $*$: $p < .001$

5 Discussion

A predominance of existing work in the area of adaptive privacy has focused on accurately predicting user preferences and behaviors [12–15, 43], without devoting enough effort to how privacy adaptations could ultimately be *presented*. Studying adaptation methods is particularly important in contexts where users do not expect a system to provide privacy advice or make decision on their behalf during the course of use.

In our study we used three adaptation methods identified by Namara et al [16]—Automation, Highlight,

and Suggestions—and examined their effectiveness in helping users better manage their privacy on an SNS platform. In this discussion section we reflect on the effect of each of these adaptation methods on users' engagement with the privacy features, their privacy protection, and their subjective evaluations.

5.1 The Effectiveness of the Adaptation Methods

Our results suggest that the **automation** of adaptations to privacy features towards stricter settings considerably increases the level of privacy protection afforded by the system and does not seem to negatively affect the level of user engagement with the privacy features.

Namara et al. [16] found that users were worried about the accuracy of the automation of the privacy features, and that automation would reduce their ability to make their own privacy decisions. They therefore suggested avoiding automatic adaptations that users' thought to be "irreversible". One interesting finding is that protection is high even when the automatic adaptations of such "irreversible" features is avoided: users seem to implement the avoided adaptations anyway, and may even issue fewer explicit rejections than if all features are automatically adapted.

Although the automatic adaptations somewhat improve users' perceived decision help and usefulness over the baseline system with no adaptations, this difference is not significant—perhaps because much of the protection happens outside of users' awareness. Another reason could be that some users still fear that the system might not be able to accurately capture their privacy preferences [16]. Indeed, Page et al. [25] assert that even when not adapted, some users are very concerned about how the use of privacy features (e.g.,untagging, unsubscribing or unfollowing a friend) hurts their relationships with others. Automation would only exacerbate the concerns of these users.

In contrast to Namara et al.'s [16] assertion that **highlights** might be able to unobtrusively raise users' awareness about privacy features, we found that this adaptation method improved neither users' level of engagement nor the overall privacy protection compared to the baseline system with no adaptations. The observed increase in subjective ratings were also not significant. This finding aligns with Warherberg et al.'s [28] assertion about the effectiveness of privacy nudges (e.g., the use of highlights) in influencing privacy decisions: they argue that the effects of some of nudges are fragile and potentially impractical for many applications. Perhaps, then, highlights should rather be used to convey and serve as indicators of new changes to an interface (e.g., to indicate a new notification or as chat/online status indicators [44]) rather than a privacy nudge or adaptation method.

Presenting adaptations to privacy features as **suggestions** results in the highest levels of engagement and relatively a high level of privacy protection. Users also found suggestions significantly more useful and helpful, but only in the condition where awkward suggestions were avoided. Namara et al. [16] assert that users appreciate suggestions as a means to increase their awareness about a privacy feature, or as a convenient shortcut to apply an adaptation without having to navigate to the feature. Our work shows that suggestions are indeed effective at increasing user engagement with privacy features, which in turn improves their privacy protection.

Namara et al.'s [16] key recommendation was that adaptation methods should be **tailored** to users' awareness and prior use of the privacy features. We find that the tailored conditions increase users' engagement (but not as much as suggestions) and protection (but not as much as automation). The tailored conditions do provide an interesting blend of *manual accept*, *explicit accept*, *implicit accept* and *implicit reject* outcomes, with very small incidences of *explicit reject*. Perhaps tailoring the adaptation methods could help strike a balance between the convenience of automation and the engagement of suggestions while avoiding their potential threats of loss control and undue burden, respectively.

5.2 Design Implications

Our results show how a variety of privacy adaptation methods can significantly improve upon the traditional SNS privacy features in different ways. Hence, which adaptation method is "best" for a certain SNS platform depends on what the designers of the platform want to accomplish? We argue that one important goal of providing privacy adaptations is **to improve users' privacy protection without causing undue burden**. In this light, we find that the **automation** of privacy feature adaptations affords users the most privacy protection without increasing or decreasing their engagement.

Whereas automations are inevitability executed by the system and can occur without explicit notification of the user, Markus and Reinhardt [45] assert that restrictive default privacy settings do not change users'

perception and enjoyment of a system (e.g., social media platform). This suggests that once users realize that an automated privacy action was executed by system on their behalf, this is not likely to change their perception about the platform. Instead, the increased privacy protection outcome is likely to alleviate their privacy concerns [45]. Thus, we recommend that if the system's objective is to drastically increase user privacy, automation or restrictive default settings should be adopted.

To decide on what features to automate, we recommend that developers automate features that would not result into unintended consequences for the user [16, 25]. We observe that avoiding the automation of certain seemingly "irreversible" privacy features does not reduce privacy protection (i.e., users will simply engage with those features manually), and may even increase protection as it makes users less likely to reject any of the adaptations.

Another important goal of providing privacy adaptations is to **encourage active ownership over one's privacy** by increasing user engagement with the available privacy features. Liu et al.'s[17] show that there tends to be a mismatch between SNS users' desired privacy settings and their actual settings, with 36% of content on social media being shared with the default settings. Our results suggest that the provision of well-timed **suggestions** can help remedy this mismatch and provide an opportunity for users to learn about the available privacy features. Under these circumstances, suggestions could be considered as a way to inform or remind users about the available privacy features in a system and the possible actions users can undertake to achieve their desired privacy setting/level. By proactively guiding users on how to appropriately safeguard their privacy, suggestions ultimately help users improve their own privacy whilst using the platform (cf. [33])—even though the protection improvements of suggestions are not as substantial as those of automation.

In line with Namara et al [16], we find it beneficial not to make suggestions for features that users would consider awkward. Although this did somewhat reduce protection and engagement (from 68% to 48%), this strategy did result in improvements in perceived decision help and perceived helpfulness—in fact, it was the only condition in which these improvements were significant.

Suggestions should also be well designed and timed. In a computer security context, Vance et al. [46] warn that constant provision of notifications is prone to habituation, which suggests that over time, users would likely stop paying attention to the suggestions. One solution would be to make the privacy suggestions stand out (with a different look and feel) from other suggestions/notifications furnished by the platform [46]. In our context, we used a virtual character ("the privacy dinosaur") to increase the salience of the suggestion and to make it more endearing.

Finally, our results show that **tailoring** adaptations to users' privacy preferences can help **strike a balance between user engagement and privacy protection**. The effect of tailoring is dependent on a wide range of parameters, so future research should further investigate how this can pragmatically be achieved.

6 Limitations

This research was primarily motivated by the earlier works of Namara et al. [16] and Colnago et al. [20]. We leveraged their insights in the development of adaptive privacy features within a working prototype of an SNS platform and examined the effects of their adaptation methods on the level of user engagement and overall privacy protection outcomes.

For experimental control purposes, we put people in the scenario, having the same goal towards managing their profile. Thus, we developed a semi-functional working prototype of an SNS platform with a fictitious profile to create an experience that was the same for all participants (safe for the adaptation method). We are cognizant that participants interactions, decisions, and subjective experiences are susceptible to the design of the site [47] and context of use [48]. Indeed, participants may have behaved differently in our prototype with another person's profile than they would on their preferred SNS using their own profile. We made the interaction with our prototype as realistic as possible to mitigate this reduction of ecological validity needed to create a feasible and carefully controlled experimental setup.

SNS platforms typically contain a plethora of privacy features. To make our study more manageable, we adopted 13 privacy features that support some of the most common privacy behaviors on SNS platforms as catalogued by Wisniewski et al. [4]. We ensured that these features kept the same core functionality as those on Facebook. As one of the goals of privacy adaptations is to support users in navigating a deluge of privacy features, we conjecture that an increase in the implemented privacy features would only strengthen our findings regarding the positive effects of the proposed adaptations.

Additionally, privacy features on social media platforms are used over time and in different contexts [48]. In our study, we used a job search-related scenario to motivate users to explore, engage, and review "their" profile. Whereas the scenario helped implore and provide rationale for users to partake in our study; users may have acted differently if this was their real profile, had used it overtime or for other scenarios.

We assessed users "use frequency" of the examined privacy features to determine the adaptation methods for the tailored experimental conditions using a subjective scale carefully crafted by Wisniewski et al [4] based on qualitative feedback. However, since there is no formal universal definition of "use frequency", participants could have had different interpretations of the term.

7 Future Work

Future work should investigate some of our surprising results, such as why highlights did not increase user engagement, despite their visual prominence. One could argue that the highlight color or size were not prominent enough to incur curiosity among users. Alternatively, users could have ignored the highlights due to a lack of explanation as to why certain privacy features were highlighted.

Finally, the design teams of social networking sites like Facebook can replicate our findings in a real-world setting, thereby investigating the feasibility and effectiveness of using the proposed adaptation methods to improve the privacy of their own social media profiles.

8 Conclusion

In this paper we examined the effectiveness of three adaptation methods—Automation, Highlights and Suggestions—in improving user engagement and overall privacy protection on an SNS platform. We find that the automation of privacy features affords users the most privacy protection, while giving privacy suggestions significantly increases their level of engagement with privacy features and improves their perceptions of helpfulness and usefulness (as long as awkward suggestions are avoided). We encourage privacy researches, designers and developers to consider these adaptation methods to help users achieve the privacy they desire.

9 Acknowledgements

We would like to thank Sai Harsha Nagabothu and Priyanka Jaiswal for their contribution towards the development of "FriendBook". We also like to thank our participants for their participation in this study. Additionally, we would also like to thank the anonyomous reviewers for their useful comments on the earlier versions of this manuscript.

Moses Namara acknowledges support from a Facebook Fellowship Award. The views and conclusions contained herein are those of the authors and should not be interpreted as representing the official policies or endorsements, either expressed or implied, of Facebook.

References

[1] D. L. Hoffman and T. Novak, "Why do people use social media? empirical findings and a new theoretical framework for social media goal pursuit," *Empirical Findings and a New Theoretical Framework for Social Media Goal Pursuit (January 17, 2012)*, 2012.

[2] P. Wisniewski, A. Islam, H. Richter Lipford, and D. C. Wilson, "Framing and measuring multi-dimensional interpersonal privacy preferences of social networking site users," *Communications of the Association for information systems*, vol. 38, no. 1, p. 10, 2016.

[3] Z. Tufekci, "Grooming, gossip, facebook and myspace: What can we learn about these sites from those who won't assimilate?" *Information, Communication & Society*, vol. 11, no. 4, pp. 544–564, 2008.

[4] P. J. Wisniewski, B. P. Knijnenburg, and H. R. Lipford, "Making privacy personal: Profiling social network users to inform privacy education and nudging," *International Journal of human-computer studies*, vol. 98, pp. 95–108, 2017.

[5] S. Hsu, K. Vaccaro, Y. Yue, A. Rickman, and K. Karahalios, "Awareness, navigation, and use of feed control settings online," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–13.

[6] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the facebook," in *International workshop on privacy enhancing technologies*. Springer, 2006, pp. 36–58.

[7] C. Kahn and D. Ingram, "Three-quarters facebook users as active or more since privacy scandal: Reuters/ipsos poll," May 2018. [Online]. Available: https://www.reuters.com/article/us-facebook-privacy-poll/three-quarters-facebook-users-as-active-or-more-since-privacy-scandal-reuters-ipsos-poll-idUSKBN1I7081

[8] M. Netter, M. Riesner, M. Weber, and G. Pernul, "Privacy settings in online social networks–preferences, perception, and reality," in *2013 46th Hawaii International Conference on System Sciences*. IEEE, 2013, pp. 3219–3228.

[9] J. Golbeck and M. L. Mauriello, "User perception of facebook app data access: A comparison of methods and privacy concerns," *Future Internet*, vol. 8, no. 2, p. 9, 2016.

[10] P. Wisniewski, A. N. Islam, B. P. Knijnenburg, and S. Patil, "Give social network users the privacy they want," in *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, 2015, pp. 1427–1441.

[11] A. Kitsiou, E. Tzortzaki, C. Kalloniatis, and S. Gritzalis, "Identifying privacy related requirements for the design of self-adaptive privacy protections schemes in social networks," *Future Internet*, vol. 13, no. 2, p. 23, 2021.

[12] B. P. Knijnenburg, "Privacy? i can't even! making a case for user-tailored privacy," *IEEE Security & Privacy*, vol. 15, no. 4, pp. 62–67, 2017.

[13] P. Bahirat, Y. He, A. Menon, and B. Knijnenburg, "A data-driven approach to developing iot privacy-setting interfaces," in *23rd International Conference on Intelligent User Interfaces*, 2018, pp. 165–176.

[14] B. Liu, M. S. Andersen, F. Schaub, H. Almuhimedi, S. A. Zhang, N. Sadeh, Y. Agarwal, and A. Acquisti, "Follow my recommendations: A personalized privacy assistant for mobile app permissions," in *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*, 2016, pp. 27–41.

[15] P. Wijesekera, A. Baokar, L. Tsai, J. Reardon, S. Egelman, D. Wagner, and K. Beznosov, "The feasibility of dynamically granted permissions: Aligning mobile privacy with user preferences," in *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2017, pp. 1077–1093.

[16] M. Namara, H. Sloan, P. Jaiswal, and B. P. Knijnenburg, "The potential for user-tailored privacy on facebook," in *2018 IEEE Symposium on Privacy-Aware Computing (PAC)*. IEEE, 2018, pp. 31–42.

[17] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing facebook privacy settings: user expectations vs. reality," in *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, 2011, pp. 61–70.

[18] R. Ravichandran, M. Benisch, P. G. Kelley, and N. M. Sadeh, "Capturing social networking privacy preferences," in *International symposium on privacy enhancing technologies symposium*. Springer, 2009, pp. 1–18.

[19] Y. He, P. Bahirat, B. P. Knijnenburg, and A. Menon, "A Data-Driven Approach to Designing for Privacy in Household IoT," *ACM Trans. Interact. Intell. Syst.*, vol. 10, no. 1, pp. 10:1–10:47, Sep. 2019. [Online]. Available: http://doi.acm.org/10.1145/3241378

[20] J. Colnago, Y. Feng, T. Palanivel, S. Pearman, M. Ung, A. Acquisti, L. F. Cranor, and N. Sadeh, "Informing the design of a personalized privacy assistant for the internet of things," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–13.

[21] D. Wilkinson, S. Sivakumar, D. Cherry, B. P. Knijnenburg, E. M. Raybourn, P. Wisniewski, and H. Sloan, "User-tailored privacy by design," in *Proceedings of the Usable Security Mini Conference*, 2017.

[22] T. B. Sheridan and W. L. Verplank, "Human and computer control of undersea teleoperators," Massachusetts Inst of Tech Cambridge Man-Machine Systems Lab, Tech. Rep., 1978.

[23] O. Pasternak, C. Veloutsou, and A. Morgan-Thomas, "Self-presentation, privacy and electronic word-of-mouth in social media," *Journal of Product & Brand Management*, 2017.

[24] O. L. Haimson, A. J. Carter, S. Corvite, B. Wheeler, L. Wang, T. Liu, and A. Lige, "The major life events taxonomy: Social readjustment, social media information sharing, and online network separation during times of life transition," *Journal of the Association for Information Science and Technology*, 2021.

[25] X. Page, R. Ghaiumy Anaraky, B. P. Knijnenburg, and P. J. Wisniewski, "Pragmatic tool vs. relational hindrance: Exploring why some social media users avoid privacy features," *Proceedings of the ACM on Human-Computer Interaction*, vol. 3, no. CSCW, pp. 1–23, 2019.

[26] Y. Wang, G. Norcie, S. Komanduri, A. Acquisti, P. G. Leon, and L. F. Cranor, "" i regretted the minute i pressed share" a qualitative study of regrets on facebook," in *Proceedings of the seventh symposium on usable privacy and security*, 2011, pp. 1–16.

[27] B. Knijnenburg, E. Raybourn, D. Cherry, D. Wilkinson, S. Sivakumar, and H. Sloan, "Death to the privacy calculus?" *Available at SSRN 2923806*, 2017.

[28] L. Warberg, A. Acquisti, and D. Sicker, "Can Privacy Nudges be Tailored to Individuals' Decision Making and Personality Traits?" in *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society*, ser. WPES'19. New York, NY, USA: Association for Computing Machinery, Nov. 2019, pp. 175–197. [Online]. Available: https://doi.org/10.1145/3338498.3358656

[29] E. Toch, J. Cranshaw, P. H. Drielsma, J. Y. Tsai, P. G. Kelley, J. Springfield, L. Cranor, J. Hong, and N. Sadeh, "Empirical models of privacy in location sharing," in *Proceedings of the 12th ACM international conference on Ubiquitous computing*, 2010, pp. 129–138.

[30] M. Benisch, P. G. Kelley, N. Sadeh, and L. F. Cranor, "Capturing location-privacy preferences: quantifying accuracy and user-burden tradeoffs," *Personal and Ubiquitous Computing*, vol. 15, no. 7, pp. 679–694, 2011.

[31] O. R. Sanchez, I. Torre, Y. He, and B. P. Knijnenburg, "A recommendation approach for user privacy preferences in the fitness domain," *User Modeling and User-Adapted Interaction*, Oct. 2019. [Online]. Available: https://doi.org/10.1007/s11257-019-09246-3

[32] L. Fang and K. LeFevre, "Privacy wizards for social networking sites," in *Proceedings of the 19th international conference on World wide web*, 2010, pp. 351–360.

[33] Y. Wang, P. G. Leon, A. Acquisti, L. F. Cranor, A. Forget, and N. Sadeh, "A field trial of privacy nudges for facebook," in *Proceedings of the SIGCHI conference on human factors in computing systems*, 2014, pp. 2367–2376.

[34] F. Schaub, B. Konings, M. Weber, and F. Kargl, "Towards context adaptive privacy decisions in ubiquitous computing," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on*. IEEE, 2012, pp. 407–410. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6197521

[35] T. B. Sheridan, "Human centered automation: oxymoron or common sense?" in *1995 IEEE International Conference on Systems, Man and Cybernetics. Intelligent Systems for the 21st Century*, vol. 1. IEEE, 1995, pp. 823–828.

[36] A. Acquisti, I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh, F. Schaub, M. Sleeper *et al.*, "Nudges for privacy and security: Understanding and assisting users' choices online," *ACM Computing Surveys (CSUR)*, vol. 50, no. 3, pp. 1–41, 2017.

[37] I. Cachola, E. Holgate, D. Preoţiuc-Pietro, and J. J. Li, "Expressively vulgar: The socio-dynamics of vulgarity and its effects on sentiment analysis in social media," in *Proceedings of the 27th International Conference on Computational Linguistics*, 2018, pp. 2927–2938.

[38] E. M. Redmiles, S. Kross, and M. L. Mazurek, "How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 1326–1343.

[39] F. Y. Kung, N. Kwok, and D. J. Brown, "Are attention check questions a threat to scale validity?" *Applied Psychology*, vol. 67, no. 2, pp. 264–283, 2018.

[40] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS quarterly*, pp. 319–340, 1989.

[41] B. P. Knijnenburg and A. Kobsa, "Making decisions about privacy: information disclosure in context-aware recommender systems," *ACM Transactions on Interactive Intelligent Systems (TiiS)*, vol. 3, no. 3, pp. 1–23, 2013.

[42] D. Thissen, L. Steinberg, and D. Kuang, "Quick and easy implementation of the benjamini-hochberg procedure for controlling the false positive rate in multiple comparisons," *Journal of educational and behavioral statistics*, vol. 27, no. 1, pp. 77–83, 2002.

[43] J. Watson, H. R. Lipford, and A. Besmer, "Mapping user preference to privacy default settings," *ACM Transactions on Computer-Human Interaction (TOCHI)*, vol. 22, no. 6, pp. 1–20, 2015.

[44] C. Cobb, L. Simko, T. Kohno, and A. Hiniker, "User experiences with online status indicators," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–12.

[45] M. Tschersich and R. Botha, "Exploring the impact of restrictive default privacy settings on the privacy calculus on social network sites," in *ECIS*, 2014.

[46] A. Vance, D. Eargle, J. L. Jenkins, C. B. Kirwan, and B. B. Anderson, "The fog of warnings: how non-essential notifications blur with security warnings," in *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, 2019.

[47] S. S. Sundar, J. Kim, M. B. Rosson, and M. D. Molina, "Online privacy heuristics that predict information disclosure," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–12.

[48] H. Nissenbaum, "A contextual approach to privacy online," *Daedalus*, vol. 140, no. 4, pp. 32–48, 2011.

A Smart Practice Example

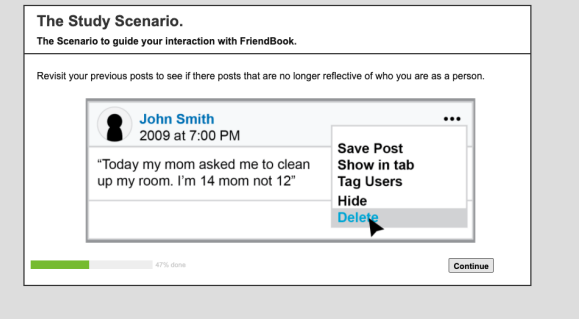

Fig. 6. An example of a smart practice used to orient and guide user interaction with FriendBook.

B Subjective Measurement Scales

Factor	Items	Loading
Perceived Decision Help from FriendBook (based on [41]) Alpha:0.83 AVE: 0.69 Correlation: 0.858	FriendBook helped me to decide how I could use the available privacy features.	0.879
	FriendBook helped me to make a tradeoff between privacy and usefulness.	0.715
	FriendBook showed me the best ways to use the available privacy features.	0.884
Perceived Usefulness of FriendBook (based on [40]) Alpha: 0.93 AVE: 0.77 Correlation: 0.858	FriendBook enabled me to use the available privacy features more quickly.	0.824
	Using FriendBook improved the quality of the decisions I made.	0.876
	FriendBook would enhance my ability to protect my privacy online.	0.909
	Overall, I found FriendBook useful in using the available privacy features.	0.921
	FriendBook would support me in being more conscious of the things I share online.	0.851

Table 2. Items used to assess participants' subjective evaluations of the FriendBook platform, along with CFA factor loadings.

C The SNS User Interface Mockup

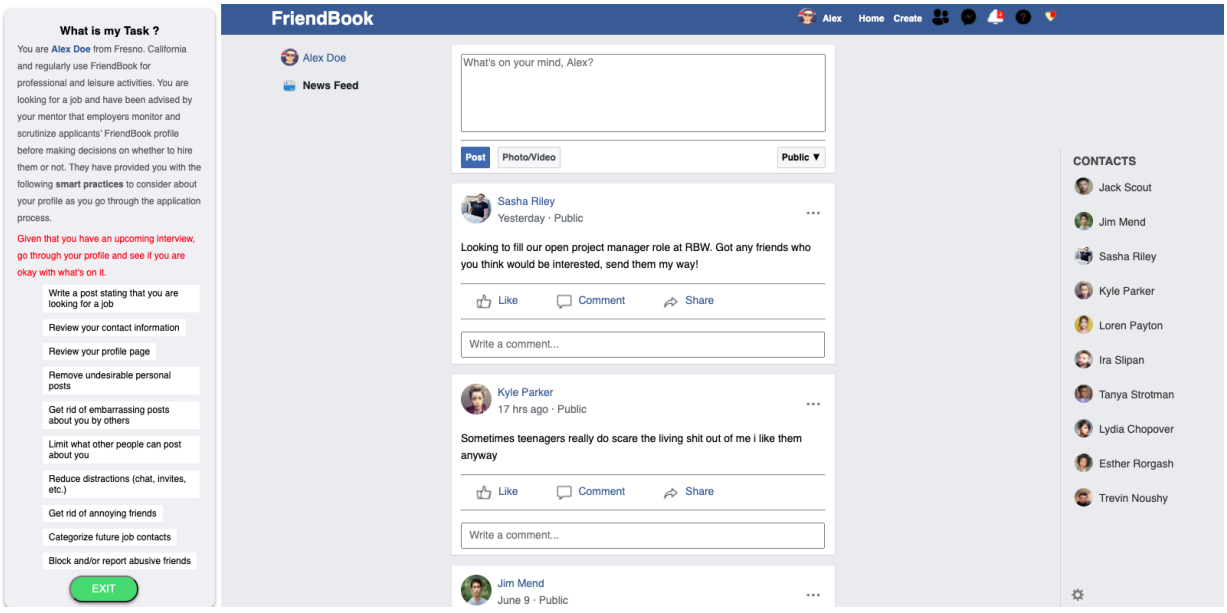

Fig. 7. The semi-functional social media platform ("FriendBook") used in exposing participants to adapted privacy features using the adaptation methods. Free public images accessed from the internet (under a (CC0) commons creative license) and fictitious names were used in the creation of "Alex Doe's" profile.

D The 13 Adapted Privacy Features

Privacy Behavior	Feature Name	Description
Altering News Feed	Hide post	Hide a post from the timeline or newsfeed.
	Unsubscribe from a friend†	Stop seeing a person's posts in the newsfeed but remain friends with them.
Selective Sharing	Audience selection	Restrict the audience that can view posts.
Timeline/Wall Moderation	Delete Post†	Delete a post.
Reputation Management	Remove Tag	Untag oneself from a post.
Restricting Chat	Changing chat availability	Turn the online chat indicator (i.e., active status) on/off.
Managing Contact Info	Contact Info	Remove contact info (e.g email, phone number, home address).
Managing Basic Info	Basic Info	Remove basic info (e.g date of birth, gender, religious/political views).
Friend Management	Organize friends	Place a friend into a custom list.
Limiting Access Control	Control who can post on timeline	Restrict the audience that can post to one's timeline.
Blocking People	Block a person*†	Stop a person from seeing one's timeline.
Blocking Apps/events	Block app invites*†	Used to block future application requests from particular friends.
	Block event invites*†	Block future event invitations requests from particular friends.

Table 3. The 13 Privacy Features adapted using the 3 adaptation methods. ∗: deemed "irreversible"; †: deemed "awkward".

E The Experimental Conditions

Conditions	Description	N
None (C1)	No adaptation is applied to any of the features.	54
$_{all}$Automation (C2)	All 13 privacy features are presented as having been automatically executed by the system.	49
$_{all}$Highlight (C3)	All 13 privacy features are highlighted using a yellow color.	45
$_{all}$ Suggestions (C4)	Suggestions are provided for all 13 privacy features.	47
$_{all}$Tailor (C5)	The adaptation method applied to each privacy feature depends on users' familiarity with and prior usage of the feature (on Facebook), as explained in Table 1.	61
$_{some}$Automation (C6)	The privacy features are presented as having been automatically executed by the system, except for the features deemed "irreversible" in Namara et al. [16] (i.e. the three Block features).	46
$_{some}$Suggestions (C7)	Suggestions are provided for the privacy features, except for the features deemed "awkward" in Namara et al. [16] (i.e., the three Block features, Delete post, and Unsubscribe from a friend).	40
$_{some}$Tailor (C8)	Like Condition C5, but automation is avoided for "irreversible" features and suggestions are avoided for "awkward" features (no adaptation is applied instead).	64

Table 4. Overview of the strategies used to adapt the 13 privacy features in each of the eight experimental conditions. Included are the number of participants (N) recruited in each condition. Note: There is no "some" variant of the Highlight condition, since Namara et al. [16] did not find any features for which its application was deemed problematic.