Privacy Support for Facebook: Empowering Users to Better Control Their Privacy

Moses Namara
Clemson University
Clemson, SC, USA
mosesn@clemson.edu

Bart P. Knijnenburg
Clemson University
Clemson, SC, USA
bartk@clemson.edu

Henry Sloan
Nyack High School
Nyack, NY, USA
henryksloan@gmail.com

Priyanka Jaiswal
Clemson University
Clemson, SC, USA
pjaiswa@clemson.edu

Abstract
Prior research has shown that Facebook users' engagement and use of privacy features greatly differs. Users' find it laborious to translate their desired privacy preferences into particular interface actions. In this study, we probe how User-Tailored Privacy (UTP) can be utilized to tailor Facebook's privacy features to user's personal preferences. Using a "think-aloud" semi-structured interview approach (N=18), we assess how three adaptation methods: *Automation, Highlight and Suggestion* can be used to suitably tailor Facebook's interface to these personal preferences. Our findings provide awareness about the viability of UTP on Facebook and other social network platforms. In particular, we find that the optimal adaptation method depends on familiar users are with the privacy feature and how they use them paired with their judgement of the awkwardness and irreversibility of the tailored privacy functionality.

Author Keywords
Privacy, user-tailored privacy, privacy on social media.

ACM Classification Keywords
K.4.1. Computers and society: Public policy issues–*privacy*.

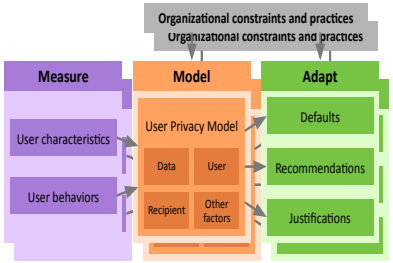

Figure 1: A schematic overview of User-Tailored Privacy.

#	Description
1	Restrict the audience that can view your photo albums
2	Block or unblock an app or game
3	Ignore future event requests from a friend
4	Block or unblock people from seeing your timeline posts
5	Place friends into custom lists
6	Turn the chat on/off
7	Add/remove your contact information
8	Restrict the audience of a post to friends on a custom list
9	Delete a post
10	Hide a post
11	Turn on/off game and app notifications and invites
12	Restrict who can look you up using your email address or phone number
13	Untag yourself from posts
14	Place friends on the "restricted" list
15	Give feedback and/or report a post
16	Limit the default audience that can view your posts
17	Restrict who can posts on your timeline, and who can see what others post on your timeline
18	Follow or unfollow a friend
19	Add/remove your personal information e.g. date of birth, languages, political views

Table 1: Description of Facebook Privacy Features tested in this study.

Introduction

There are quite a number of privacy controls and features available on Facebook that users can use to protect their privacy [19]. While these features are certainly extensive, research has shown that users privacy preferences are vastly different [18, 20],they find it laborious to translate their desired privacy preferences towards particular interface actions [11], and often do not pester with the available and accessible controls despite their desire to control their private information[3].

User-Tailored Privacy practitioners recommend automatically tailoring a platforms privacy settings to the user's privacy preferences [7] to make it easier for users to manage their privacy and overall find the right fit between their desire for privacy and actual experiences [19]. The successful implementation of user-tailored privacy features is not a simple undertaking[6]. However, presuming its possibility, we are left with two important research questions: *which* features should be tailored to the user's preferences (**RQ1**) and *how* should such adaptations be implemented (**RQ2**)? To find answers to these research questions, we used a think-aloud approach and interviewed 18 participants to learn of their reactions to user-tailored versions of 19 Facebook privacy features. Each of the privacy features was implemented in the 3 versions of the adaptation methods: *Automation*, *Highlight* and *Suggestion.*

Related Work

Facebook Users' Privacy Behaviors

Prior work has shown that Facebook users vastly differ in how they control their privacy, often engage different privacy protection mechanisms [20], and that their experience can be enhanced if a right fit between the protection offered by the platform and their privacy needs is achieved [19]. Nevertheless, users often fail to effectively manage their privacy on social networks [10, 11, 15] including as their privacy decisions are often influenced by heuristic factors such as the design and appearance of a website [1, 6]. While researchers have developed various ways to increase the transparency and control of the privacy functionalities of social network sites[2, 5, 8, 14], often users find the privacy notices too long, obscure and incomprehensible . As a result they generally avoid the hassle of really exerting control over their data including whether it is monetized or deleted [13, 3].

User-Tailored Privacy (UTP)

Knijnenburg et al. [6] define UTP as an approach that provides decision support by first *measuring* users' privacy preferences and behaviors, using the measurements to create a personalized *model* and finally *adapting* the user interface to the predicted privacy preferences by changing the default privacy settings (Figure 1). It can be utilized to make users' privacy decision-making easier. User preferences and behaviors can be drawn from personal and contextual factors such as the data requested ("what"), user("who"), system ("whom") [16 4] for the *measure* part while for the *model* part several researches such as Wisniewski et al. [20] investigated the dimensionality of the privacy behaviors of 308 Facebook users, extracted 11 behavioral strategies upon which they clustered users. They found 6 privacy management profiles: Privacy Maximizers, Selective Sharers, Privacy Balancers, Self-Censors, Time Savers/Consumers and Privacy Minimalists.

Figure 2: Mockup of the Automation version of feature 13 "untag yourself from posts".

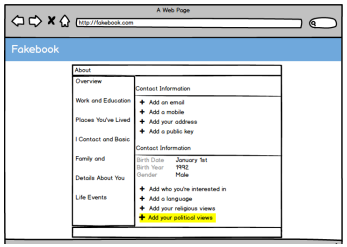

Figure 3: Mockup of the Highlight version of feature 19: "Add/remove personal information e.g. date of birth, language, political views".

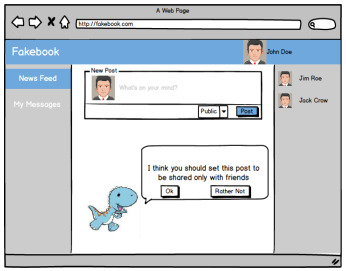

Figure 4: Mockup of the Suggestion version of feature 8: "restrict the audience of a post to friends on a custom list".

Testing Adaptation Methods

Few works have carefully examined and tested the *adapt* part of UTP [6][17].These have shown that adaptations are generally welcomed by users . For example, Liu et al. [9] found that 78.7% of recommendations made by a personalized privacy assistant in a field study were adopted by users. What optimum adaptation method can utilized in tailoring the platforms privacy features?- is the open question [6] we attempted to answer in this work.

Methodology

We designed 19 paper mockups of "user-adaptive" versions of Facebook privacy features (Table 1). Each of the privacy features was implemented in the 3 versions of the adaptation methods: *Automation*, *Highlight* and *Suggestion* to help showcase the different degrees of automation based on the need for user input, some user input or no user input at all. The participants were presented with the paper prototypes and implored to provide their opinions on the adaptive capabilities and suitable of the three adaptation methods. Eighteen participants were semi-structurally interviewed and each compensated with a $5 Starbucks gift card.

Automation

The Automation adaptation method (Figure 2) enables interface and feature adaptations without any permission request or user action. This adaptation method offers the highest degree of automation as it potentially can accrue outside the user's awareness unless if they are notified about its occurrence. In our implementation, the user is not explicitly notified of the automatic adaptation but is rather able to learn of its occurrence only if they navigate to the spot where they normally would have undertaken the action themselves.

Highlight

The Highlight adaptation method (Figure 3) requires moderate user action. It increases the visual prominence and or leads the user to the action that the system predicts the user would want to take. This can be done either through a color change, or by giving the recommended action a more prominent location within the platform. In our implementation, the recommended action is highlighted yellow. The Highlight method implements a moderate degree of automation: it gives users a clear indication as to what action they should consider thus reducing their cognitive *load* without reducing their *control given they have the option to either ignore the highlight or pursue on it* [12].

Suggestion

The Suggestion adaptation method (Figure 4) uses an "agent" (virtual character) to suggest a recommended action for the user to take. Our implementation is based on Facebook's "Privacy Dinosaur", which the Facebook platform currently uses to display "Privacy Check-up" notifications to the user. The Dinosaur provides suggestions in a general form of, "I think you should...", increasing the personal nature of the interaction [12]. The provided options are "Ok" and "Rather Not", allowing the user to either accept or reject the recommended action. Users were told that if they selected "Ok", the setting would automatically be changed however they would still be taken to the appropriate setting as well. By asking for an explicit decision and user action, this adaptation method implemented our lowest degree of automation.

Awkward/ Irreversible?	Awareness/Usage?		
	Unfamiliar/ Do not use	*Occasional use*	*Frequent use*
Yes	As is	Highlight	As is
No	Suggestion	Highlight	Automation

Table 2: Preferred Adaptation Methods given adaptation effects and user privacy feature awareness or usage.

Findings and Discussion

Our findings detailed in [12] and summarized in Table I answer and shed an interesting light on our research questions. We find that the preferred adaptation method for the different privacy features depends on users' awareness and usage of those features (RQ2). Since different Facebook users are (un)familiar with different features, this means that the preferred adaptation method for each feature differs per user. The adaptation method itself should thus be tailored to the user as well. Moreover, we find that the preferred adaptation method may sometimes not be suitable, in which case users end up preferring the untailored version (RQ1). This limits the extent to which user-tailored privacy can be implemented on Facebook.

Unfamiliar/Infrequently-Used Features

Facebook users prefer suggestions for privacy features they are largely unfamiliar with[12]. In addition, our implementation of Suggestion (and with use of the "Privacy Dinosaur") provides the opportunity to explain the adaptive behavior and learn about new privacy features in a more engaging way. These explanations help reduce the cognitive load involved in making privacy decisions.

Occasionally Used Features

Facebook users prefer Highlights for features they occasionally use because they are easily made aware of any new changes[12]. This is a compromise in preference as suggestions would be a distraction for more especially for regularly used features and also be intrusive if they show up too frequently. Automation on the other hand would significantly reduce control as users would not be as familiar with the features to be comfortable enough with the system to automatically making a decision on their behalf.

Frequently-Used Features

Users prefer Automation for features they frequently use [12]. Frequent users already know what to do with a feature, so their main effortful load is rather physical than cognitive. Thus, neither Highlight nor Suggestion would sufficiently reduce this load. Users also seem to have an intuitive understanding that their frequent use of a feature likely improves the quality of the adaptive behavior. This gives them a certain amount of 'indirect' control over the Automation method. However, users do not prefer the Automation method when the resulting automated privacy decision feels irreversible.

Limitations and Future Work

Our study relied on user's self-reported evaluation of a limited subset of prominent Facebook privacy features that were mere paper adaptive feature mockups, using cartoon style renderings with less visually distracting features as compared to the actual Facebook. This might have given them a less realistic appearance but made it easier for participants to concentrate on the presented adaptation mechanisms. In future work, researchers, developers and designers can leverage our findings to develop adaptive privacy features in research prototypes or real-world social networking sites.

Conclusion

Our results demonstrate the viability and contribute to the advancement of UTP. We believe that our insights will help researchers, designers and developers in their future endeavors developing user-tailored privacy interfaces and experiences

References

[1] Acquisti, A. and Grossklags, J. 2008. What Can Behavioral Economics Teach Us About Privacy? *Digital Privacy: Theory, Technologies, and Practices*. A. Acquisti et al., eds. Auerbach Publications. 363–377.

[2] Church, L. et al. 2009. Privacy Stories: Confidence in Privacy Behaviors Through End User Programming. *Proceedings of the 5th Symposium on Usable Privacy and Security* (Mountain View, CA, 2009).

[3] Compañó, R. and Lusoli, W. 2010. The Policy Maker's Anguish: Regulating Personal Data Behavior Between Paradoxes and Dilemmas. *Economics of Information Security and Privacy* (New York, NY, 2010), 169–185.

[4] Dong, C. et al. 2015. Predicting Privacy Behavior on Online Social Networks. *Ninth International AAAI Conference on Web and Social Media* (Apr. 2015), 91–100.

[5] Kelley, P.G. et al. 2010. Standardizing privacy notices: an online study of the nutrition label approach. *Proceedings of the 28th International Conference on Human Factors in Computing Systems* (Atlanta, Georgia, 2010), 1573–1582.

[6] Knijnenburg, B.P. et al. 2017. Death to the Privacy Calculus? *Proceedings of the 2017 Networked Privacy Workshop at CSCW* (Portland, OR, Feb. 2017).

[7] Knijnenburg, B.P. 2017. Privacy? I Can't Even! Making a Case for User-Tailored Privacy. *IEEE Security Privacy*. 15, 4 (2017), 62–67. DOI:https://doi.org/10.1109/MSP.2017.3151331.

[8] Lipford, H.R. et al. 2008. Understanding Privacy Settings in Facebook with an Audience View. *Proceedings of the 1st Conference on Usability, Psychology, and Security* (Berkeley, CA, USA, 2008).

[9] Liu, B. et al. 2016. Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions. *Twelfth Symposium on Usable Privacy and Security* (Denver, CO, Jun. 2016), 27–41.

[10] Liu, Y. et al. 2011. Analyzing facebook privacy settings: user expectations vs. reality. *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement* (New York, NY, USA, 2011), 61–70.

[11] Madejski, M. et al. 2012. A study of privacy settings errors in an online social network. *Fourth International Workshop on Security and Social Networking* (Lugano, Switzerland, 2012), 340–345.

[12] Namara, M. et al. 2018. The Potential for User-Tailored Privacy on Facebook [Under Review].

[13] Nissenbaum, H. 2011. A Contextual Approach to Privacy Online. *Daedalus*. 140, 4 (Oct. 2011), 32–48. DOI:https://doi.org/10.1162/DAED_a_00113.

[14] Raber, F. et al. 2016. Privacy Wedges: Area-Based Audience Selection for Social Network Posts. *Twelfth Symposium on Usable Privacy and Security* (Denver, CO, Jun. 2016).

[15] Strater, K. and Lipford, H.R. 2008. Strategies and struggles with privacy in an online social networking community. *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers* (Swinton, UK, 2008), 111–119.

[16] Wang, Y. et al. 2011. "I regretted the minute I pressed share": a qualitative study of regrets on Facebook. *Proceedings of the Seventh Symposium on Usable Privacy and Security* (Pittsburgh, PA, 2011), 10:1–10:16.

[17] Wilkinson, D. et al. 2017. User-Tailored Privacy by Design. *Proceedings of the Usable Security Mini Conference* (San Diego, CA, 2017).

[18] Wisniewski, P. et al. 2016. Framing and Measuring Multi-dimensional Interpersonal Privacy Preferences of Social Networking Site Users. *Communications of the Association for Information Systems*. 38, 1 (Jan. 2016). DOI:https://doi.org/10.17705/1CAIS.03810.

[19] Wisniewski, P. et al. 2015. Give Social Network Users the Privacy They Want. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Vancouver, Canada, 2015), 1427–1441.

[20] Wisniewski, P.J. et al. 2017. Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of Human-Computer Studies*. 98, (Feb. 2017), 95–108. DOI:https://doi.org/10.1016/j.ijhcs.2016.09.006.