POSTER: Design ideas for privacy-aware user interfaces for mobile devices

Neel Tailor
De Montfort University
Leicester, LE9 1BH, UK
n.ee.l@live.co.uk

Ying He
De Montfort University
Leicester, LE9 1BH, UK
ying.he@dmu.ac.uk

Isabel Wagner
De Montfort University
Leicester, LE9 1BH, UK
isabel.wagner@dmu.ac.uk

ABSTRACT

Privacy in mobile applications is an important topic, especially when it concerns applications that gather and process health data. Using MyFitnessPal as an example eHealth app, we analyze how privacy-aware its user interface is, i.e. how well users are informed about privacy and how much control they have. We find several issues with the current interface and develop five design ideas that make the interface more privacy-aware. In a small pilot user study, we find that most of the design ideas seem to work well and enhance end users' understanding and awareness of privacy.

Categories and Subject Descriptors

H.5.2 [**Information Interfaces and Presentation**]: User Interfaces; K.4.1 [**Computers and Society**]: Public Policy Issues—*privacy*

General Terms

Design, Human Factors, Security

Keywords

privacy awareness, mobile applications, user interface design

1. INTRODUCTION

With the increasing use of eHealth apps and their unprecedented access to sensitive data, eHealth privacy has become an important concern to the public. User interfaces (UIs) provide the point of contact between users and apps, and ideally allow users to express their privacy preferences towards apps. However, current eHealth app UIs have not been designed in a privacy-aware manner, which stops users from making informed and effective privacy choices [3]. Existing efforts to improve the privacy communication between apps and users focus on improving awareness of privacy policies and app permissions before an app is installed [1, 2]. In contrast, we consider the privacy-awareness of user interfaces while the user is using the app.

WiSec'16, July 18 - 20, 2016, Darmstadt, Germany

DOI: http://dx.doi.org/XX.XXXX/XXXXXXX.XXXXXXX.

MyFitnessPal is an eHealth app that allows users to track food consumption, exercise and body weight, thus supporting users in achieving their dieting goals. We use MyFitnessPal as an example to analyze weaknesses in the privacy awareness of current mobile user interfaces. Based on this analysis, we develop a privacy enhanced prototype UI and evaluate whether it helps users become more aware of their privacy and make more informed privacy decisions. While we developed the prototype to improve MyFitnessPal's UI, we are confident that our ideas are applicable to other mobile device UIs as well. Our research has implications for app designers who need to consider how to communicate privacy issues to their users throughout the design and development phases, building usable privacy into apps.

2. CRITERIA FOR UI DESIGN

We follow the three stages of the Inform–Alert–Mitigate (I-AM) cycle [3] to analyze MyFitnessPal's current user interface. The I-AM cycle is a user-centric approach to systematically assess and improve how privacy issues are addressed during app usage. The *inform* stage informs users of potential privacy issues, for example using privacy policies and app permission requests. The *alert* stage alerts users to ongoing privacy risks, for example caused by data transfers or sensor usage. The *mitigate* stage gives users options to mitigate ongoing privacy risks, for example by blocking data transfers or modifying sensor readings.

3. ANALYSIS OF CURRENT UI

For the *inform* stage, we find that lengthy privacy policies packed with legalese are not suitable for educating eHealth consumers on data collection, usage and sharing. In addition, links to privacy policies are presented so that users may not even notice them. For the *alert* stage, we find that users have no way to find out about ongoing data transfers or sensor usage. In addition, the on-screen alerts that ask users for specific permissions do not help users in deciding how much this permission will affect their privacy. For the *mitigate* stage, we find that users have no concrete mitigation options, other than uninstalling the app. Specifically, apps do not offer users to store data locally on the device, or to disable specific sensors.

4. DESIGN IDEAS TO ADDRESS GAPS

To overcome the issues with current user interfaces that we identified above, we developed a set of five design ideas that can be implemented into mobile user interfaces.

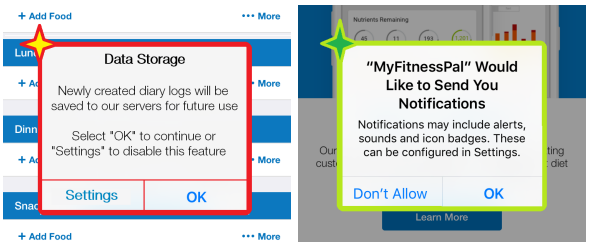

Figure 1: Traffic light alerts

Privacy Policy. We re-structured the privacy policy by separating statements in the policy into different categories: information collection, information use, information sharing, user control over stored information, service operation, and notification of policy changes. Each category is displayed with clear headings and icons that can be expanded by the user (Fig. 2). In addition to restructuring, we make display of the privacy policy mandatory before the app is first used. This is in contrast to how privacy policies are currently handled on app stores, where apps can be installed without ever seeing the privacy policy.

Icons for sensor usage. Icons for accelerometer usage and data transfers (top two items in Fig. 3) help to alert users to ongoing privacy risks. While using the app, these icons are displayed in the phone's status bar, similar to the already existing GPS icon, whenever data transfers are ongoing or sensors are being used.

Traffic light colors for alerts. We integrated a traffic light color scheme into on screen alerts that are displayed to the user (Fig. 1). The alerts are color-coded as red, amber, or green depending on the severity of the privacy notification. The color-coding enhances visual privacy awareness and ensures users pay more attention to more severe alerts.

Mitigation options. We designed an easily accessible mitigation options menu that the user can access during app usage (Fig. 3). The menu allows users to disable specific sensors the eHealth app uses, and to stop data transfers to the eHealth organization's remote servers. This concrete mitigation feature allows users to configure the data that eHealth apps acquire from them, thus giving users more control over their privacy, as well as increasing user trust and confidence in eHealth applications.

Incognito mode. The incognito mode ensures data is stored locally (bottom item in Fig. 3) by disabling data transfers to the app provider's servers and instead stores data locally on the device. This allows a person to freely use the eHealth app without having to worry that their data could be retrieved at a later date or shared with third parties.

5. EVALUATION

The user study involved providing the privacy enhanced prototype app as well as the original MyFitnessPal app to a sample of 16 people, who were then asked a series of questions about the new privacy features. The results show that the restructured privacy policy is easy to follow and more engaging than the current display of privacy policies. In addition, presenting the privacy policy before first use of the app increases the likelihood that it will be read. Almost all of our participants agreed that the new icons for data transfers

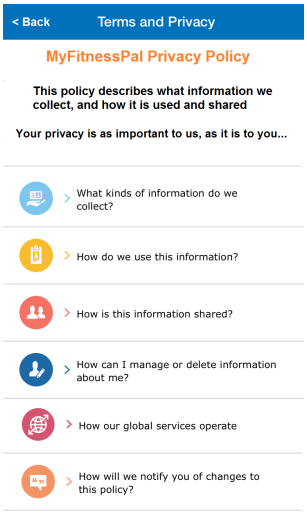

Figure 2: Privacy policy

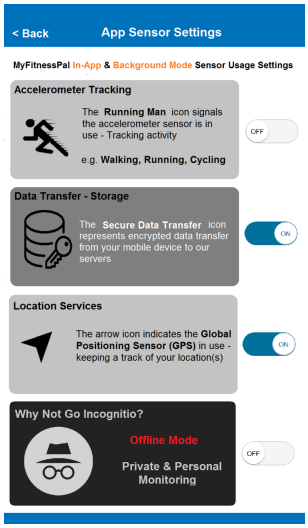

Figure 3: Settings

and sensor usage made them more aware of the resources the app was using. More than 90% of the participants approved of our traffic light color scheme integrated into the on-screen alerts, and all agreed that they were better alerted to the severity of ongoing privacy risks. Over 80% of the participants found that the mitigation menu was easily accessible throughout the app, and the concept of having this menu gave almost all participants more control over their privacy and meant that they could tailor the app to their desires. The incognito mode was not as successful as the other ideas. Less than 50% of participants stated that they could use the app more confidently and felt their privacy would not be compromised. This may be caused by the wording we displayed when enabling incognito mode, because it did not clarify that data gathered during incognito mode would stay local and not be uploaded at any time.

6. CONCLUSIONS

This research found five issues with the current interface of the mobile eHealth app MyFitnessPal and developed five design ideas to address them. The results show that most of the design ideas help to enhance users' understanding and awareness of privacy. In our future research, we will seek to gather eHealth app providers' perspectives and involve more users in the evaluation for a further proof of concept. Our long term goal is to expand and refine our design ideas and integrate them into a fully functional application.

7. REFERENCES

[1] P. G. Kelley, L. F. Cranor, and N. Sadeh. Privacy As Part of the App Decision-making Process. In *CHI '13*, pages 3393–3402, Paris, France, 2013. ACM.

[2] J. Lin, S. Amini, J. I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang. Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy Through Crowdsourcing. In *UbiComp '12*, pages 501–510, Pittsburgh, PA, USA, 2012. ACM.

[3] I. Wagner, Y. He, D. Rosenberg, and H. Janicke. User Interface Design for Privacy Awareness in eHealth Technologies. In *CCNC '16*, pages 38–43, Las Vegas, NV, January 2016. IEEE.