Privacy Notifications for Transparency in Fitness Apps

Mirco Baseniak[a], Tom Lorenz[b] and Ina Schiering[c]
Faculty of Computer Science, Ostfalia University of Applied Sciences, Wolfenbüttel, Germany

Keywords: Fitness App, mHealth, Privacy, Privacy Notification, User Study.

Abstract: mHealth applications including fitness apps are an important trend. To monitor fitness activities a broad range of personal data is processed typically including location data and vital signs. For some of these applications it is not transparent which data is processed. To foster transparency and intervenability in mobile applications the concept of privacy notifications is an opportunity to provide users with information about processed data during the use of the application. In the context of a fitness app a concept for privacy notifications is proposed and evaluated in a user study.

1 INTRODUCTION

The use of fitness apps and digital platforms for motivating and monitoring physical activities is a significant trend during the last years (Salzwedel et al., 2017; Armstrong and Richter, 2021; Shaw et al., 2021). Especially during the pandemic the use of such mHealth applications gained importance (Parker et al., 2021). Beside the use of fitness apps in the context of leisure activities, the use in healthcare is promoted by recent legal regulations as the digital care act in Germany, that allows physicians to prescribe certified health apps to patients (Heidel and Hagist, 2020).

Mulder (Mulder, 2019) analyzed privacy policies of health apps and emphasized that it is difficult to get concrete information about the processing of personal data from these policies. Based on the investigation of network communication of health apps Grundy et al. (Grundy et al., 2017) analyzed data flows based on organizational structures including app families and social media networks and reported significant security and privacy issues.

To foster transparency concerning processing of personal data and privacy beside static data protection policies also dynamic concepts as for example privacy dashboards were proposed (Murmann and Fischer-Hübner, 2017; Raschke et al., 2017) which focus on visualizing processing of personal data and data transfers for applications on computers. For mobile applications and especially apps which act as companions in daily activities such as sports, a privacy dashboard could be nevertheless helpful. But since personal data as location data and potentially also vital signs are collected and processed on a permanent basis additional notifications could remind users of their configuration concerning data processing. In the context of mobile health applications the concept of privacy notifications was proposed by Murmann (Murmann, 2019) to foster transparency. A privacy notification notifies users about personal data processing which is considered relevant for them and is typically triggered in the context of an event.

Based on this general approach of privacy notifications a concept for fitness apps based on the user interface of the open source fitness app OpenTracks is developed. The perception of users concerning usability of the proposed privacy notifications was investigated in the context of an anonymous online user study where a usage scenario and accompanying questionnaires are employed.

2 RELATED WORK

Despite the fact that health-related information is considered as sensitive data, mHealth applications incorporate significant security and privacy issues (Papageorgiou et al., 2018). For fitness apps, location data is a central basis for activity tracking. Especially location data poses the risk of re-identification of individuals based on specific locations as place of residence, workplace resp. locations of schools, etc. Privacy

[a] https://orcid.org/0000-0003-2599-864X
[b] https://orcid.org/0000-0001-9594-7683
[c] https://orcid.org/0000-0002-7864-5437

Baseniak, M., Lorenz, T. and Schiering, I.
Privacy Notifications for Transparency in Fitness Apps.
DOI: 10.5220/0010912600003123
In *Proceedings of the 15th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2022) - Volume 5: HEALTHINF*, pages 705-710
ISBN: 978-989-758-552-4; ISSN: 2184-4305

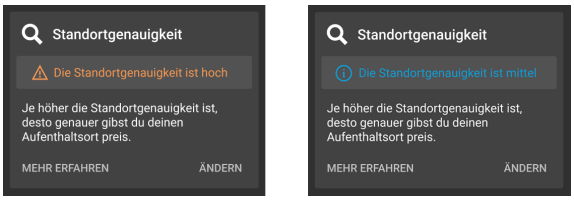

Figure 1: Examples of privacy notifications concerning location accuracy representing different criticalities, i.e. warning and information.

risks of location data and approaches for addressing these risks are broadly investigated (Krumm, 2009; Primault et al., 2019). The use of mobile devices and fitness and health apps are already investigated in several studies incorporating also privacy concerns of users (Wiesner et al., 2018; Shaw et al., 2021).

Although users state that they have privacy concerns, they are not willing to take adequate countermeasures and accept often privacy risks in the context of concrete applications (Vervier et al., 2017). This so called privacy paradox (Coopamootoo and Groß, 2017) expresses the divergence between privacy attitudes and privacy behavior.

Beyond static privacy policies several approaches were investigated to foster transparency of processing of personal data during the use of the application and allow for intervenability by users (Murmann and Fischer-Hübner, 2017). Since in the context of mobile applications the usability of such dashboards is limited, in this context privacy notifications were proposed (Murmann, 2019; Jackson and Wang, 2018). Although this is in general a promising approach such notifications are often perceived as annoying by users (Micallef et al., 2017).

Hence to address privacy concerns of users, the concept of privacy notifications is be considered as an interesting privacy enhancing technology fostering transparency. In the context of a case study it could be investigated which amount of notifications is considered as helpful or annoying.

3 CONCEPT FOR PRIVACY NOTIFICATIONS

The concept for privacy notifications proposed here is based on the user interface of the open source fitness app OpenTracks[1]. We suppose that a typical fitness app processes the following types of data and allows to share this data e.g. with a physician or a trainer:

- type of activity
- duration of activity
- distance
- speed
- location data (GPS)
- vital signs

Data sharing implies typically that the corresponding data is synchronized with a cloud service. Specific aspects concerning this cloud service are not considered here. The focus is on privacy notifications.

Since users prefer to be informed concerning all stated categories but on the other hand a huge amount of notifications is not considered helpful (Murmann, 2019) and notifications have only a low priority for users (Micallef et al., 2017), the number of notifications should be restricted. To end this, the notifications need to be in a casual relation to an activity and should be triggered at the beginning of an activity or after an activity. It is assumed that the attention to additional information of users at the beginning of an activity is low when the information is not directly associated with intended activity, notifications are triggered after the activity. Some types of privacy notifications could be deactivated by users.

Privacy notifications (see Figure 1) present the subject, then the criticality (e.g. warning, information) is visualized by an icon and a short text in a color associated with the criticality. Afterwards a summary of the notification is presented and users are able to choose whether they want more detailed information or change the configuration concerning this aspect. To allow users to review privacy notifications also later, to get an overview about data processing and transfer in the context of past activities and intervene by changing configurations, an overview of past privacy notifications can be reviewed by users (see Figure 2).

4 METHODOLOGY OF THE USER STUDY

To evaluate the concept of privacy notifications in a user study, study participants followed a given usage scenario in an online web application which presents screen shots and asks for predefined interaction accompanied by anonymous questionnaires. Participants were provided a link to the web application and questionnaires which could be used on their smartphones, tablets ot computers online via a web browser. Before the start they were provided with an information sheet about the study. There was no remuneration for participants.

[1] https://opentracksapp.com/

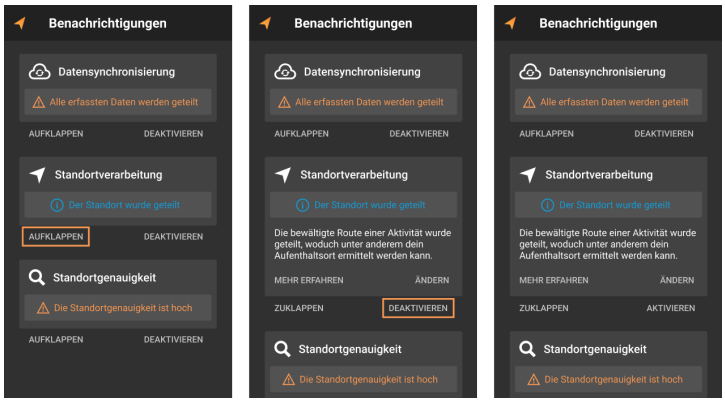

Figure 2: Overview of past privacy notifications about data synchronization, location tracking and location accuracy, buttons for detailed information and deactivating specific privacy notifications are highlighted.

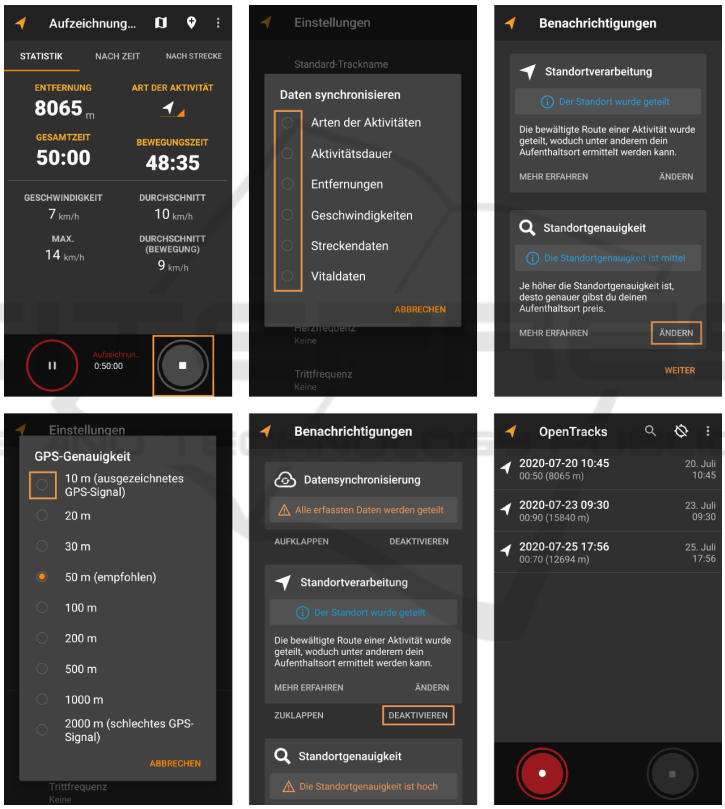

Figure 3: Excerpt from the scenario showing a screen shot of tracking during running activity, configuration of data synchronization, privacy notifications, configuration of location accuracy, deactivation of specific privacy notifications and an overview about tracked activities.

The structure of the anonymous online study consisting of a scenario and corresponding questionnaires is summarized in the following:

1. Online questionnaire concerning demographic data, technical competencies and the frequency of sporting activities, the use of fitness trackers and the general privacy perception.
2. Introduction of users to the scenario: The general scenario and the context is described. Also the interaction with the web application is explained. Intended interaction with buttons or check boxes is highlighted by orange rectangles.
3. Users follow the web-based scenario: A runner tracks sporting activities on a regular basis. To this end the tracking during activities and changes

of configuration are presented. In a *tracking phase* users start tracking and several screen shots show that the user is running a certain amount of time. Afterwards the user stops the tracking and a screen with an overview is presented. In addition privacy notifications are shown where applicable. In *configuration phases* based on screen shots users configure the processing of personal data and data synchronization with an external service. Users experience the following phases (see Figure 3):

(a) Tracking without data synchronization (no privacy notifications)
(b) Configuration of data synchronization with an external service
(c) Tracking with data synchronization (privacy notifications about data synchronization including location and location accuracy)
(d) Configuration of privacy notifications (deactivation of one notification)
(e) Tracking with additional smart watch (privacy notifications about data synchronization of vital signs and location accuracy)

4. Online questionnaire: Usability of privacy notification based on System usability scale (SUS) (Brooke et al., 1996).
5. Online questionnaire: Users should report whether they feel distracted, supported by the notifications, if they are understandable and if the point in time and the frequency are considered adequate.
6. Online questionnaire: Users should state which configuration of data synchronization and accuracy of location tracking they would have chosen.

The time needed to follow the scenario and answer the questionnaires is approximately 30 minutes for participants.

5 RESULTS

5.1 Demographics of Participants

Participants for the user study were recruited among sports groups, students and in the personal environment. 51 persons started the study, but only 27 (53%) completed the whole study. It can be assumed that this reflects the relatively high amount of time needed. Since participation was online and anonymous, it was not possible to ask for specific reasons why they did not finish the study. There were 20 (74%) male and 7 (26%) female participants.

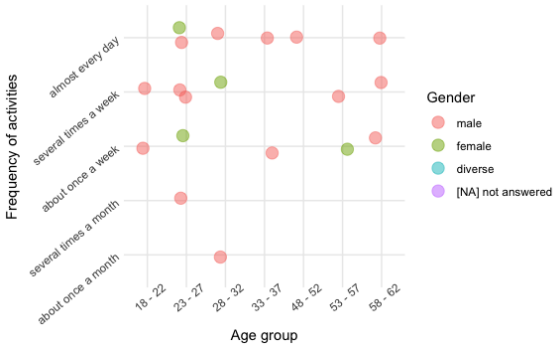

Figure 4: Frequency of activities and age.

The majority of participants 70% (19/27) reported to perform sporting activities on a regular basis. Figure 4 gives an overview of gender, age and frequency of sporting activities of these 19 participants. The frequency of sporting activities ranges between once per month and almost every day. On average participants do sports several times per week. Among the participants performing sports 79% (15/19) use a fitness app and 74% (14/19) also a smart watch. Concerning the importance of privacy ranging from 1 *not important* to 5 *very important*, participants reported the following (see Table 1):

Table 1: Importance of privacy as stated by participants.

importance of privacy	number of participants
1 (not important)	0
2 (slightly important)	5
3 (moderately important)	10
4 (important)	10
5 (very important)	2

5.2 Perception of Privacy Notifications

The participants reported on average that privacy notification were understandable and the perceived distraction was relatively low. Most of the participants (17/27) considered the notifications as in general helpful. They stated short texts are preferred that are easily understandable. Figure 5 gives an overview of the perceived support from the privacy notifications, gender and sporting activities.

In addition, the general usability of the privacy notifications presented in the scenario was measured with the SUS questionnaire (Brooke et al., 1996). The SUS score evaluated according to (Bangor et al., 2009) is 68,8% which is there considered as *good*.

That privacy notifications were triggered after the activity was in general perceived as reasonable. Figure 6 gives an overview of the distribution of the an-

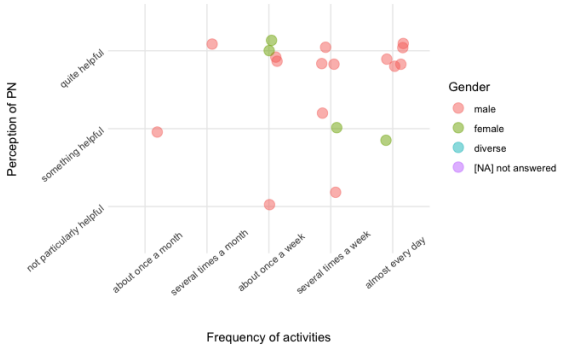

Figure 5: Perception of privacy notifications.

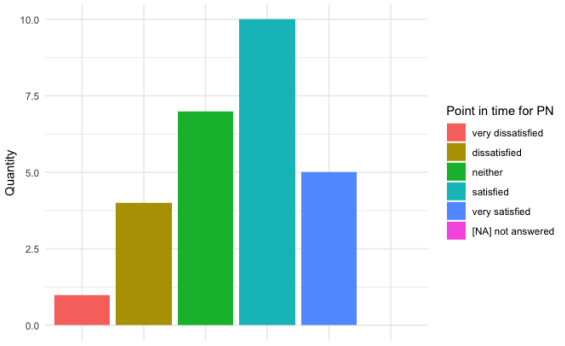

Figure 6: Point in time for privacy notifications.

swers and shows that a wide range of opinions was determined here. As alternative points in time it was proposed to trigger them a certain period after the activity e.g. after a shower. Since fitness apps are used beside tracking of activities also for the reviewing of activities also this was proposed as an alternative point in time for triggering privacy notifications since there is more time to read them.

Participants reported also on average that the amount of notifications was considered slightly too much. The range of answers was between *far too much* and *adequate*, whereas no participants stated that there were insufficiently many notifications. Participants that consider privacy important in general perceive the amount of privacy notifications as adequate.

Concerning the subjects of privacy notifications 41% (11/27) wanted to be informed about unknown personal data, 59% (16/27) about sensitive personal data, 37% about all personal data and 26% (7/27) about all data which is processed.

According to the questions after the scenarios about how the participants would configure data synchronization themselves, 74% (20/27) would share the type of activity, 81% (22/27) the duration of the activity, 81% (22/27) the distance, 78% (21/27) information about speed, 67% (18/27) location data and 59% (16/27) information about vital signs. Concerning the accuracy of location tracking (13/27) would stick to 50m (recommended) whereas (12/27) would prefer maximal accuracy (10m).

6 DISCUSSION AND CONCLUSION

The user study shows that the proposed concept of privacy notifications was in general perceived as helpful in the context of fitness apps.

Although participants were interested in a broad range of privacy related information, the amount of notifications was in general considered as a critical factor. Hence privacy notifications should be easily configurable and mainly information concerning critical aspects should be presented per default. To be perceived as helpful the text of privacy notifications needs to be concise and understandable for a broad range of users. Additional details can be presented on demand. The principle task of the application (e.g. fitness monitoring) must still be in the focus of the user.

Privacy notifications have great potential to foster transparency and intervenability in the context of mobile applications and wearables. The results of this study are in line with general usability investigations in this area (Micallef et al., 2017). The contribution of the presented study is the investigation in the specific usage scenario fitness monitoring which corresponds with users personal interests. To address the gap between privacy attitude and privacy perception the study was based on a typical usage scenario. In addition further investigations based on implementations would be interesting.

REFERENCES

Armstrong, M. and Richter, F. (2021). Infographic: Smartphone as personal trainer. https://www.statista.com/chart/24702/gcs-share-smartphone-users-regularly-use-fitness-apps/ [Last accessed on 2021-11-08].

Bangor, A., Kortum, P., and Miller, J. (2009). Determining what individual sus scores mean: Adding an adjective rating scale. *Journal of Usability Studies*, 4(3):114–123.

Brooke, J. et al. (1996). Sus-a quick and dirty usability scale. *Usability evaluation in industry*, 189(194):4–7.

Coopamootoo, K. P. and Groß, T. (2017). Why privacy is all but forgotten. *Proc. Priv. Enhancing Tech-*

nol., 2017(4):97–118. https://doi.org/10.1515/popets-2017-0040.

Grundy, Q., Held, F. P., and Bero, L. A. (2017). Tracing the potential flow of consumer data: A network analysis of prominent health and fitness apps. *Journal of Medical Internet Research*, 19(6):e7347. https://doi.org/10.2196/jmir.7347.

Heidel, A. and Hagist, C. (2020). Potential benefits and risks resulting from the introduction of health apps and wearables into the german statutory health care system: Scoping review. *JMIR mHealth and uHealth*, 8(9):e16444. https://doi.org/10.2196/16444.

Jackson, C. B. and Wang, Y. (2018). Addressing the privacy paradox through personalized privacy notifications. *Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies*, 2(2):1–25. https://doi.org/10.1145/3214271.

Krumm, J. (2009). A survey of computational location privacy. *Personal and Ubiquitous Computing*, 13(6):391–399. https://doi.org/10.1007/s00779-008-0212-5.

Micallef, N., Just, M., Baillie, L., and Alharby, M. (2017). Stop annoying me! an empirical investigation of the usability of app privacy notifications. In *Proceedings of the 29th Australian Conference on Computer-Human Interaction*, pages 371–375. https://doi.org/10.1145/3152771.3156139.

Mulder, T. (2019). Health apps, their privacy policies and the gdpr. *European Journal of Law and Technology*, 10(1).

Murmann, P. (2019). Eliciting design guidelines for privacy notifications in mhealth environments. *International Journal of Mobile Human Computer Interaction (IJMHCI)*, 11(4):66–83. https://doi.org/10.4018/IJMHCI.2019100106.

Murmann, P. and Fischer-Hübner, S. (2017). Tools for achieving usable ex post transparency: A survey. *IEEE Access*. https://doi.org/10.1109/ACCESS.2017.2765539.

Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., and Patsakis, C. (2018). Security and privacy analysis of mobile health applications: The alarming state of practice. *IEEE Access*, 6:9390–9403. https://doi.org/10.1109/ACCESS.2018.2799522.

Parker, K., Uddin, R., Ridgers, N. D., Brown, H., Veitch, J., Salmon, J., Timperio, A., Sahlqvist, S., Cassar, S., Toffoletti, K., Maddison, R., and Arundell, L. (2021). The use of digital platforms for adults' and adolescents' physical activity during the covid-19 pandemic (our life at home): Survey study. *Journal of Medical Internet Research*, 23(2):e23389. https://doi.org/10.2196/23389.

Primault, V., Boutet, A., Mokhtar, S. B., and Brunie, L. (2019). The long road to computational location privacy: A survey. *IEEE Communications Surveys Tutorials*, 21(3):2772–2793. https://doi.org/10.1109/COMST.2018.2873950.

Raschke, P., Küpper, A., Drozd, O., and Kirrane, S. (2017). *Designing a GDPR-compliant and usable privacy dashboard*, pages 221–236.

Salzwedel, A., Rabe, S., Zahn, T., Neuwirth, J., Eichler, S., Haubold, K., Wachholz, A., Reibis, R., and Völler, H. (2017). User interest in digital health technologies to encourage physical activity: Results of a survey in students and staff of a german university. *JMIR mHealth and uHealth*, 5(4):e7192. https://doi.org/10.2196/mhealth.7192.

Shaw, M. P., Satchell, L. P., Thompson, S., Harper, E. T., Balsalobre-Fernández, C., and Peart, D. J. (2021). Smartphone and tablet software apps to collect data in sport and exercise settings: Cross-sectional international survey. *JMIR mHealth and uHealth*, 9(5):e21763. https://doi.org/10.2196/21763.

Vervier, L., Zeissig, E.-M., Lidynia, C., and Ziefle, M. (2017). Perceptions of digital footprints and the value of privacy. In *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security - Volume 1: IoTBDS,*, pages 80–91. INSTICC, SciTePress. https://doi.org/10.5220/0006301000800091.

Wiesner, M., Zowalla, R., Suleder, J., Westers, M., and Pobiruchin, M. (2018). Technology adoption, motivational aspects, and privacy concerns of wearables in the german running community: field study. *JMIR mHealth and uHealth*, 6(12):e201. https://doi.org/10.2196/mhealth.9623.