Participatory Design Study about Privacy Enhancing Technologies for Wearable Activity Tracker Data Sharing

Noé Zufferey[1], Kavous Salehzadeh Niksirat[1,2], Mathias Humbert[1], Kévin Huguenin[1]
[1] *University of Lausanne, Switzerland*
[2] *EPFL, Switzerland*

Abstract

Wearable activity tracker users (WAT) lack knowledge about data-sharing. Furthermore, most of them are not fully aware of their own data-sharing behavior. It is, therefore, crucial to design privacy-enhancing technologies (PETs) to help them better manage their data-sharing, and therefore, protect their privacy. In this article, we explore how a participatory design approach can be used to design PETs, together with the users. We conducted three design sessions with 8-9 different users in each session. During these sessions, the participants had to propose and evaluate new PETs related to WAT data sharing. The outcome of these sessions was 19 different designs that we then categorized into seven different categories of functionalities. We then evaluated these different functionalities regarding their feasibility, effectiveness, adoption, and usability as PETs. Finally, we propose a general solution implementing the different functionalities with the best evaluation scores.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.
August 6–8, 2023, Anaheim, CA, USA

1 Introduction

Wearable activity tracker (WAT) data are generally kept on the user's device or on the service provider's cloud. But it may also be shared voluntarily by users with other individuals and entities, typically through third-party applications (TPAs). Users do so for increased social or financial benefits (e.g., better projection of the self, decreased insurance premiums) and/or for additional features not offered by the original services or application. However, they may lose track of their TPAs [16], or some TPAs may collect more data than they need to provide their services [12], share them with other parties, and/or use them against the users' consent.

Previous research has shown that WAT users tend to adopt risky data-sharing behavior due to their lack of awareness and understanding of the WAT data-sharing ecosystem [19].

Therefore, it is crucial to set up privacy-enhancing technologies (PETs) to help the users better manage and keep track of their multiple applications and better understand how the fitness-data sharing ecosystem works, and thus, avoid risky behaviors for privacy, such as sharing more data than is actually required or not regularly checking the previously granted permissions to revoke them if necessary. Few studies, evaluated the potential for adoption of such PETs (i.e., related to TPAs) [17, 19], and some others developed PETs in the context of WAT data sharing [1, 2, 4, 5, 6, 7, 15, 16, 18]. However, for these studies, the tools are designed by the researchers, and none of them uses a user-centric approach.

We report the results obtained by conducting a participatory design study with WAT users (N=26).

2 Methodology

Participatory design is a user-centric design approach that allows designers to include the end-users in the process of the design [9], such approach has been used in multiple studies related to utility (including WAT utility) [3, 10, 11] or privacy [8, 14].

We recruited 26 WAT users in total to conduct 3 participatory design sessions with 8-9 participants for each session.

During each session, we briefly introduced what data sharing is (what can be shared and to whom) and then asked the participants some thought-provoking questions in order to raise the problem of privacy. Then, we presented what are the potential threats to privacy caused by WAT data-sharing. We then together reconstructed the WAT data-sharing ecosystem and presented what is the current literature knowledge about users' behavior and understanding of data-sharing with third parties. Next, after briefly giving the users a few tips about design, we set up discussions (in small groups) on how to improve users' understanding of the whole data-sharing ecosystem, awareness of their own behavior, and develop multiple solutions. The outcome of these sessions is PETs that aim to assist WAT users in the data-sharing process, and therefore, protect their privacy. The form of solutions were storyboards or low-fidelity paper prototypes. After this sketching session (70 minutes) every design was presented to all the participants and was evaluated on a 5-point Likert Scale regarding four points: feasibility (i.e., do they think it is feasible to develop), effectiveness (i.e., would it be effective to protect the users' privacy), usability (i.e., would the user interface be easy to be used) and adoption (i.e., would WAT users use the solution in everyday life).

After all the sessions, we collected 19 drawings representing the participants' designs (each group submitted two designs except for one group who submitted three). Then, we used open coding [13] to categorize the multiple functionalities included in the different designs. Then, the categories were presented to the two remaining authors, and all authors evaluated every category regarding the same four criteria previously described.

3 Results

We extracted seven different PET categories from the 19 designs collected during the participatory design sessions: (1) Sharing only part of the data, (2) Transparency & Visualization, (3) Reminders and Notifications, (4) TPAs limit, (5) Centralization & Verification, (6) Sensitization, Education, and (7) TPA's mobile app uninstallation/access revocation assistance. After having classified and evaluated the various proposed functionalities that can help users better manage their data-sharing and increase their privacy, we can claim that a general solution implementing functionalities from Category 1, 3, and 7 would be a particularly interesting tool to help WAT users increase their privacy.

New functionalities such as allowing the user to select which data they want to share regarding the time it was collected could indeed address one major misunderstanding regarding data sharing. Furthermore, it could highly increase privacy by substantially reducing the amount of data that a potential adversary would have access to.

Mechanisms such as reminder notifications and "opt-out" or "opt-in" access authorization renewal were also evaluated as being highly usable and effective. As the feasibility of such a solution is particularly high, it should be taken into account. However, the user should be able to choose the frequency of such notifications or to disable them, for example by checking a box appearing together with the notification (e.g., "don't ask me again").

Finally, functionalities to help users revoke data access when uninstalling a TPA's mobile app or to ask TPA's company to remove data from their servers received the most positive feedback from the participants and from the experts. Therefore, we can claim that such a protection mechanism should be implemented.

References

[1] Angeliki Aktypi, Jason R.C. Nurse, and Michael Goldsmith. Unwinding Ariadne's Identity Thread: Privacy Risks with Fitness Trackers and Online Social Networks. In *Proc. of the Multimedia Privacy and Security (MPS)*, pages 1–11, New York, NY, USA, October 2017. Association for Computing Machinery. ZotAbbreviate:no proceedingsTitle;.

[2] Abdulmajeed Alqhatani and Heather R. Lipford. Exploring The Design Space of Sharing and Privacy Mechanisms in Wearable Fitness Platforms. In *Workshop on Usable Security and Privacy (USEC)*, 2021.

[3] SR Davis, D Peters, RA Calvo, SM Sawyer, JM Foster, and L Smith. "Kiss myAsthma": Using a participatory design approach to develop a self-management app with young people with asthma. *Journal of Asthma*, 55(9):1018–1027, September 2018. Publisher: Taylor & Francis _eprint: https://doi.org/10.1080/02770903.2017.1388391.

[4] Jaco du Toit. PAUDIT: A Distributed Data Architecture for Fitness Data. In Hein Venter, Marianne Loock, Marijke Coetzee, Mariki Eloff, and Jan Eloff, editors, *Information and Cyber Security (Communications in Computer and Information Science)*, pages 43–56, Cham, 2020. Springer International Publishing. ZotAbbreviate:no proceedingsTitle;.

[5] Daniel A. Epstein, Alan Borning, and James Fogarty. Fine-grained sharing of sensed physical activity: a value sensitive approach. In *UbiComp*, pages 489–498, New York, NY, USA, September 2013. Association for Computing Machinery. ZotAbbreviate:no proceedingsTitle;.

[6] Kambiz Ghazinour, Emil Shirima, Vijayasimha Reddy Parne, and Abhilash BhoomReddy. A Model to Protect Sharing Sensitive Information in Smart Watches. *Procedia Computer Science*, 113:105–112, January 2017.

[7] Yanmin Gong, Yuguang Fang, and Yuanxiong Guo. Private data analytics on biomedical sensing data via distributed computation. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 13(3):431–444, May 2016.

[8] Alethia Hume, Nicolás Ferreira, and Luca Cernuzzi. The design of a privacy dashboard for an academic environment based on participatory design. In *2021 XLVII Latin American Computing Conference (CLEI)*, pages 1–10, October 2021.

[9] Finn Kensing and Andreas Munk-Madsen. PD: structure in the toolbox. *Communications of the ACM*, 36(6):78–85, June 1993.

[10] Stephen Lindsay, Daniel Jackson, Guy Schofield, and Patrick Olivier. Engaging older people using participatory design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, pages 1199–1208, New York, NY, USA, May 2012. Association for Computing Machinery.

[11] Meethu Malu and Leah Findlater. Toward Accessible Health and Fitness Tracking for People with Mobility Impairments. In *Proceedings of the 10th EAI International Conference on Pervasive Computing Technologies for Healthcare*, Cancun, Mexico, 2016. ACM.

[12] Mehdi Nobakht, Yulei Sui, Aruna Seneviratne, and Wen Hu. PGFit: Static permission analysis of health and fitness apps in IoT programming frameworks. *Journal of Network and Computer Applications*, 152:102509, February 2020.

[13] Johnny Saldana. *The Coding Manual for Qualitative Researchers*. SAGE Publishing, Thousand Oaks, California, 4th ed edition, 2021. tex.ids= saldana_coding_2021-1 googlebooksid: RwcVEAAAQBAJ.

[14] Kavous Salehzadeh Niksirat, Evanne Anthoine-Milhomme, Samuel Randin, Kévin

Huguenin, and Mauro Cherubini. “I thought you were okay”: Participatory Design with Young Adults to Fight Multiparty Privacy Conflicts in Online Social Networks. In *Designing Interactive Systems Conference 2021*, pages 104–124, Virtual Event USA, June 2021. ACM.

[15] Odnan Ref Sanchez, Ilaria Torre, Yangyang He, and Bart P. Knijnenburg. A recommendation approach for user privacy preferences in the fitness domain. *User Modeling and User-Adapted Interaction*, 30(3):513–565, July 2020.

[16] Ilaria Torre, Odnan Ref Sanchez, Frosina Koceva, and Giovanni Adorni. Supporting users to take informed decisions on privacy settings of personal devices. *Personal and Ubiquitous Computing*, 22(2):345–364, April 2018.

[17] Lev Velykoivanenko, Kavous Salehzadeh Niksirat, Noé Zufferey, Mathias Humbert, Kévin Huguenin, and Mauro Cherubini. Are Those Steps Worth Your Privacy?: Fitness-Tracker Users’ Perceptions of Privacy and Utility. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 5(4):1–41, December 2021.

[18] Jing Wang, Na Wang, and Hongxia Jin. Context Matters? How Adding the Obfuscation Option Affects End Users’ Data Disclosure Decisions. In *Proc. of the Int’l Conf. on Intelligent User Interfaces (IUI)*, pages 299–304, New York, NY, USA, March 2016. Association for Computing Machinery. ZotAbbreviate:no proceedingsTitle;.

[19] Noé Zufferey, Kavous Salehzadeh Niksirat, Mathias Humbert, and Kévin Huguenin. "Revoked just now!" Users’ Behaviors Toward Fitness-Data Sharing with Third-Party Applications. *Proc. on Privacy Enhancing Technologies (PoPETs)*, 2023(1):47–67, January 2023.