User-Centered Privacy to Improve User Quantification using Smartphone Sensing

Florian Bemmann
LMU Munich
Munich, Germany
florian.bemmann@ifi.lmu.de

ABSTRACT

Mobile sensing technologies enable adaptive and context-aware applications. At the same time, they raise a range of privacy concerns. Thus, to reduce privacy concerns today apps are restricted from accessing certain information hindering to deliver full personalization and novel adaptive use cases. I investigate this issue by shedding light on the privacy concerns that arise from state-of-the-art mobile sensing data, studying the users' perspective on mobile smartphone privacy, and proposing concepts that protect the users' privacy while keeping the resulting data usable. I found that there is a lack of user-centered privacy design and that control features play a key role to give the users more agency. My results motivate the proliferation of control-enhancing privacy features in mobile applications. I show that the benefits of trust and system adoption surpass any impairments that control features might bring to the data.

CCS CONCEPTS

• **Human-centered computing → Human computer interaction (HCI)**.

KEYWORDS

human computer interaction

ACM Reference Format:
Florian Bemmann. 2023. User-Centered Privacy to Improve User Quantification using Smartphone Sensing. In *25th International Conference on Mobile Human-Computer Interaction (MobileHCI '23 Companion), September 26–29, 2023, Athens, Greece.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3565066.3609737

1 INTRODUCTION

Ubiquitous and mobile technology tracks various kinds of user behavior data, e.g., mobile behavior [30], location [31], and physiological data [27]. These tracking features make it possible to build adaptive and intelligent user interfaces providing the user with information right when they are needed, e.g., [22]. On the other hand, the concerns of users about privacy in mobile sensing apps are often disregarded, and user-friendly solutions for privacy-friendly data usage are rare cf. [15]. The great variety and amount of ubiquitous data makes it hard to give the user transparency and control (c.f. [8, 13, 18]). Users can only hardly estimate what can be inferred from raw sensing data [16], and furthermore, the passive sensing approach that mobile sensing follows has, due to its unobtrusiveness, additional privacy risks as users do hard grasping what actually happens in the background.

Such privacy issues can lead to users' data being used against them (e.g., [24]) and pose real-world security risks. Also, the fear of privacy issues leads to reduced user trust, diminishing the system's adoption rates (e.g., in the context of research applications [19, 21, 29]). At the same time, smartphone sensing enables a brought range of applications, which can support the user, e.g., [32]. Current systems either live with these issues or significantly throttle their data collection, which hinders some of their intended use cases.

With my thesis, I want to give users more transparency and control over their sensing data. Thereby an important aspect of my thesis is not to do this by solely limiting data access to applications, as this obstructs many novel application scenarios which themselves would be for their users' good. Instead, the privacy-enhancing technologies I envision realize the sweet spot of the least necessary data. Thereby privacy is protected, while developers are not obstructed. At the beginning of my thesis, I start off by studying what information can be extracted from the user with mobile sensing systems, and which use cases thereby can be pursued (e.g. [6, 34]). I shed light on the privacy issues that come with such state-of-the-art mobile sensing systems, putting an emphasis on the users' perspective on mobile smartphone privacy and their envisioned mitigation measures. By proposing approaches that enable privacy-friendly use of ubiquitous mobile sensing data, I inform the design of mobile applications that on the one hand have fewer privacy concerns among users, and on the other hand, thereby allowing developers to use sensing data for novel use cases, that would not have been usable privacy-wise beforehand (e.g., [5, 7]). Past systems mostly approached privacy issues by limiting the amount of data that is released to applications. While this successfully improves privacy, unfortunately, the advancements in adaptive and context-aware applications are thereby throttled, which finally is not in the users' interest.

During my research, I found a general lack of user-centered privacy design, as pure technical protection measures have a limited impact on user trust and privacy perception. Transparency and control thereby are the central user desires that need to be met. Of especially importance is thereby control: While an increase in transparency initially increases users' privacy concerns, they can be mitigated by offering users control features on the data logging. The crucial point thereby is the sole availability of the control features, their actual use by the users has been rather low

MobileHCI '23 Companion, September 26–29, 2023, Athens, Greece

ACM ISBN 978-1-4503-9924-1/23/09.
https://doi.org/10.1145/3565066.3609737

in our studies. Our results motivate application developers to include more transparency and especially control features in their mobile sensing applications. Our results have shown that control availability increases trust, reduces privacy concerns, and leads to higher system adoption. The associated impairment of the data is relatively low, as users only rarely make actual use of the control features.

2 RESEARCH OBJECTIVE AND STATUS

My thesis structures into three parts: In the first part, I investigate what information can be extracted from the user with state-of-the-art mobile sensing systems. In the second part, I point out the thereby emerging privacy risks, focusing on the user perspective. In the third part, I then propose three approaches that reduce the privacy invasiveness of mobile sensing technology while keeping the output that fuel's the data's use case.

2.1 Extracting Information from the User with Mobile Sensing Systems

Exploring the Mobile Phone Rabbit Hole. We leveraged a mobile sensing app to study the mobile phone rabbit hole on smartphones. With a mixed methods approach consisting of both experience sampling and passive sensing data, we characterize rabbit hole sessions, and how the users perceive this predominant phenomena. Our paper, which has been accepted for MobileHCI'23 [34], thereby shows how mobile sensing can be used for user-centered research and to understand how users use and perceive their mobile devices. Furthermore, we envision adaptive interface concepts that help users cope with the rabbit hole phenomena when needed.

Mobile Typing Language Data. In a project following a huge mobile sensing field study, we investigate which hidden potential lies in mobile typing language metadata. We show that field hint texts reveal a lot about the text inputs' context and intention. We envision that to be either used as a data source in psychological and sociological research, as well as a means to filter language data more accurately than the current approach of filtering by app category does. This can be done on-device easily and helps to implement the principle of data minimization.

Intent Prediction. In our future work, we will next focus on deep app usage data, i.e., detailed information on what users are doing in an app and what contents apps show. We see the potential for novel adaptive UI use cases here, like predicting the user's intent and thereby delivering information right when it is needed. This data comes with severe privacy implications, which is the reason for it not being used yet despite accessibility use cases. Thus, better privacy concepts than the current ones are needed.

2.2 Emerging Privacy Issues: The User Perspective

To get insights into what the smartphone privacy situation looks like from the users' perspective, we are currently conducting a set of qualitative studies. Finding out what users really are concerned about, which real-world consequences they fear happening, and what solutions could mitigate the issues is an important basis to design more user-centered privacy-enhancing technologies.

2.3 How can we improve that privacy-wise, without obstructing the data usability

On-Device Preprocessing of Mobile Typing Language Data. Data preprocessing on the user's device is a good measure to realize data minimization. Only the necessary information should leave the device. Therefore we developed an on-device text abstraction concept, that allows privacy-friendly analysis of mobile typing behavior for research purposes. In a paper published in the EICS journal [5], we propose a concept consisting of on-device word categorization, frequency counting, and regular expression matchers, implemented as an Android keyboard application. In a user study, we found that people especially appreciate the word categorization as a privacy-preserving concept. We have analyzed the effectiveness of our approach in a theoretical experiment, where we investigate the thresholds from which it becomes unlikely for a language model to reconstruct the original raw content.

The Influence of Transparency and Control Features. With progressing automation, keeping the user in the loop of their data becomes evermore important [16]. Transparency and control features are the two key measures to implement this [16]. We studied the effects of offering users (a) transparency and (b) control features in a mobile sensing app on a.o. perceived privacy, system adoption, and trust. In a user study, which is published at MobileHCI'22 [7], we found that transparency initially worsened the user perspective (reduced trust, significantly lower app adoption rate). However adding control to the system mitigated and even outpassed this effect, leading to higher perceived privacy and more people using the app. Interestingly from the developer perspective, we found that the sole presence of the control features makes the difference. In fact, these features were only very rarely used.

A Continuous Smartphone Permission Concept. In future work, I plan to study UI concepts that give users more fine-grained control over their data. The current "all or nothing" approach in the smartphone permission systems does not allow the user the express their desires and thereby does not enable apps to leverage the full potential of mobile sensing data. We envision that detailed smartphone usage data could become usable for novel adaptive systems: In the example of Android, such data is only available through accessibility services. As they enable access to nearly everything that the user does on their phone, it is allowed to use it only for very specific purposes for privacy reasons. We envision that if there were intermediate options between giving away all data and none at all, such data could be used for more use cases in the future.

3 RELATED WORK

Various studies exist on user privacy perception (e.g. [17, 20, 26]) and how that translates to behavior (e.g. [1, 4, 25]). The research concludes that privacy issues are the most important barriers to app adoption [9, 10, 12] and points out the importance to put users in the loop [16, 28]. However, existing privacy-enhancing systems in mobile sensing systems lack clarifying privacy implications, and users behave inconsistently with their concerns Christin et al. [11].

There is a general lack of research on smartphone privacy from the user perspective [9, 10, 12] as deep insights on underlying user concerns are rather a byproduct [14].

Privacy-enhancing technologies are often studied rather technically [11, 23], and have issues from the user perspective. The existence of technical protection measures does not necessarily lead to trust and reduced concern. Furthermore, smartphone permission systems have to deal with the tradeoff between warning fatigue and user control [33], and some extent of user ignorance [2, 3].

Alternative approaches to smartphone privacy exist, for example, Scoccia et al. [33] proposing more fine-grained permissions on smartphones and Zhou et al. [35] who give users more control over the data that is given to the system. Again this work is rather technical and lacks evaluation of effects on the users. Also, the effects of transparency and control features on the user and the data are understudied. While research exists in domains such as webshops and the personalization of online services [36], literature coping with mobile sensing data is rare and contradictory [17].

4 RESEARCH SITUATION AND EXPECTED CONTRIBUTION

I am currently a 5th year Ph.D. student at the LMU Munich and envision finishing my Ph.D. within the next year. I contribute to mobile sensing methodology and user-centered privacy concepts on mobile devices. The contributions are not only valuable in HCI to inform future privacy-enhancing interface concepts but also for interdisciplinary research in psychology and sociology that use mobile sensing as a data source for their studies.

ACKNOWLEDGMENTS

I would like to thank Heinrich Hussmann, who allowed me to get started with all this but passed away too early, and Sven Mayer who took over my supervision and is always present with great guidance and support.

REFERENCES

[1] Alessandro Acquisti and Jens Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE Security Privacy* 3, 1 (2005), 26–33. https://doi.org/10.1109/MSP.2005.22

[2] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your Location Has Been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 787–796. https://doi.org/10.1145/2702123.2702210

[3] Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen. 2013. "Little Brothers Watching You": Raising Awareness of Data Leaks on Smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (Newcastle, United Kingdom) *(SOUPS '13)*. Association for Computing Machinery, New York, NY, USA, Article 12, 11 pages. https://doi.org/10.1145/2501604.2501616

[4] Susanne Barth, Menno DT de Jong, Marianne Junger, Pieter H Hartel, and Janina C Roppelt. 2019. Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and informatics* 41 (2019), 55–69. https://doi.org/10.1016/j.tele.2019.03.003

[5] Florian Bemmann and Daniel Buschek. 2020. LanguageLogger: A Mobile Keyboard Application for Studying Language Use in Everyday Text Communication in the Wild. *Proc. ACM Hum.-Comput. Interact.* 4, EICS, Article 84 (jun 2020), 24 pages. https://doi.org/10.1145/3397872

[6] Florian Bemmann, Carmen Mayer, and Sven Mayer. 2023. Leveraging Mobile Sensing Technology for Societal Change Towards more Sustainable Behavior. In *Workshop Proceedings of the HCI for Climate Change: Imagining Sustainable Futures* (2023-04-23) *(HCI4CC23)*. https://doi.org/10.48550/arXiv.2303.12426 arXiv:2303.12426 [cs.HC]

[7] Florian Bemmann, Maximiliane Windl, Jonas Erbe, Sven Mayer, and Heinrich Hussmann. 2022. The Influence of Transparency and Control on the Willingness of Data Sharing in Adaptive Mobile Apps. *Proc. ACM Hum.-Comput. Interact.* 6, MHCI, Article 189 (sep 2022), 26 pages. https://doi.org/10.1145/3546724

[8] Jan Hendrik Betzing, Matthias Tietz, Jan vom Brocke, and Jörg Becker. 2020. The impact of transparency on mobile privacy decision making. *Electronic Markets* 30, 3 (2020), 607–625. https://doi.org/10.1007/s12525-019-00332-3

[9] Jan Blom, Daniel Gatica-Perez, and Niko Kiukkonen. 2011. People-Centric Mobile Sensing with a Pragmatic Twist: From Behavioral Data Points to Active User Involvement. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services* (Stockholm, Sweden) *(MobileHCI '11)*. Association for Computing Machinery, New York, NY, USA, 381–384. https://doi.org/10.1145/2037373.2037431

[10] Mauro Cherubini, Rodrigo de Oliveira, Anna Hiltunen, and Nuria Oliver. 2011. Barriers and Bridges in the Adoption of Today's Mobile Phone Contextual Services. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services* (Stockholm, Sweden) *(MobileHCI '11)*. Association for Computing Machinery, New York, NY, USA, 167–176. https://doi.org/10.1145/2037373.2037400

[11] Delphine Christin, Andreas Reinhardt, Salil S Kanhere, and Matthias Hollick. 2011. A survey on privacy in mobile participatory sensing applications. *Journal of systems and software* 84, 11 (2011), 1928–1946. https://doi.org/10.1016/j.jss.2011.06.073

[12] Christos Efstratiou, Ilias Leontiadis, Marco Picone, Kiran K Rachuri, Cecilia Mascolo, and Jon Crowcroft. 2012. Sense and sensibility in a pervasive world. In *International Conference on Pervasive Computing*. Springer, Cham, 406–424. https://doi.org/10.1007/978-3-642-31205-2_25

[13] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the eighth symposium on usable privacy and security*. 1–14. https://doi.org/10.1145/2335356.2335360

[14] Alisa Frik, Juliann Kim, Joshua Rafael Sanchez, and Joanne Ma. 2022. Users' expectations about and use of smartphone privacy and security settings. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–24. https://doi.org/10.1145/3491102.3517504

[15] Paul Gerber, Melanie Volkamer, and Karen Renaud. 2015. Usability versus Privacy Instead of Usable Privacy: Google's Balancing Act between Usability and Privacy. *SIGCAS Comput. Soc.* 45, 1 (feb 2015), 16–21. https://doi.org/10.1145/2738210.2738214

[16] Gabriella M Harari. 2020. A process-oriented approach to respecting privacy in the context of mobile phone tracking. *Current opinion in psychology* 31 (2020), 141–147. https://doi.org/10.1016/j.copsyc.2019.09.007

[17] Sabrina Karwatzki, Olga Dytynko, Manuel Trenz, and Daniel Veit. 2017. Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems* 34, 2 (2017), 369–400. https://doi.org/10.1080/07421222.2017.1334467

[18] Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. 2012. A conundrum of permissions: installing applications on an android smartphone. In *International conference on financial cryptography and data security*. Springer, 68–79. https://doi.org/10.1007/978-3-642-34638-5_6

[19] Florian Keusch, Bella Struminskaya, Christopher Antoun, Mick P Couper, and Frauke Kreuter. 2019. Willingness to participate in passive mobile data collection. *Public opinion quarterly* 83, S1 (2019), 210–235. https://doi.org/10.1093/poq/nfz007

[20] Predrag Klasnja, Sunny Consolvo, Tanzeem Choudhury, Richard Beckwith, and Jeffrey Hightower. 2009. Exploring privacy concerns about personal sensing. In *International Conference on Pervasive Computing*. Springer, 176–183. https://doi.org/10.1007/978-3-642-01516-8_13

[21] Frauke Kreuter, Georg-Christoph Haas, Florian Keusch, Sebastian Bähr, and Mark Trappmann. 2020. Collecting survey and smartphone sensor data with an app: Opportunities and challenges around privacy and informed consent. *Social Science Computer Review* 38, 5 (2020), 533–549. https://doi.org/10.1177/0894439318816389

[22] Florian Künzler. 2019. Context-aware notification management systems for just-in-time adaptive interventions. In *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. IEEE, 435–436. https://doi.org/10.1109/PERCOMW.2019.8730874

[23] Jialiu Lin, Bin Liu, Norman Sadeh, and Jason I Hong. 2014. Modeling Users' Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX Association, 199–212. https://doi.org/10.5555/3235838.3235856

[24] Sandra C Matz, Michal Kosinski, Gideon Nave, and David J Stillwell. 2017. Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the national academy of sciences* 114, 48 (2017), 12714–12719.

[25] Patricia A Norberg, Daniel R Horne, and David A Horne. 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs* 41, 1 (2007), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

[26] Iryna Pentina, Lixuan Zhang, Hatem Bata, and Ying Chen. 2016. Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior* 65 (2016), 409–419.

[27] Sarah Prange, Sven Mayer, Maria-Lena Bittl, Mariam Hassib, and Florian Alt. 2021. Investigating User Perceptions Towards Wearable Mobile Electromyography. In *Human-Computer Interaction – INTERACT 2021*. Springer International Publishing, Cham, 339–360. https://doi.org/10.1007/978-3-030-85610-6_20

[28] Emilee Rader. 2022. Normative and Non-Social Beliefs about Sensor Data: Implications for Collective Privacy Management. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 653–670. https://www.usenix.org/conference/soups2022/presentation/rader

[29] Melanie Revilla, Mick Couper, and Carlos Ochoa. 2019. Willingness of Online Panelists to Perform Additional Tasks. *methods, data, analyses* 13, 2 (2019), 29. https://doi.org/10.12758/mda.2018.01

[30] Alireza Sahami Shirazi, Niels Henze, Tilman Dingler, Martin Pielot, Dominik Weber, and Albrecht Schmidt. 2014. Large-Scale Assessment of Mobile Notifications. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 3055–3064. https://doi.org/10.1145/2556288.2557189

[31] Albrecht Schmidt, Michael Beigl, and Hans Gellersen. 1999. There is more to context than location. *Computers & Graphics* 23, 6 (1999), 893–901. https://doi.org/10.1016/S0097-8493(99)00120-X

[32] Ramona Schoedel, Fiona Kunz, Maximilian Bergmann, Florian Bemmann, Markus Bühner, and Larissa Sust. 2023. Snapshots of daily life: Situations investigated through the lens of smartphone sensing. *Journal of Personality and Social Psychology* (2023). https://doi.org/10.1037/pspp0000469

[33] Gian Luca Scoccia, Ivano Malavolta, Marco Autili, Amleto Di Salle, and Paola Inverardi. 2019. Enhancing trustability of android applications via user-centric flexible permissions. *IEEE Transactions on Software Engineering* 47, 10 (2019), 2032–2051.

[34] Nađa Terzimehić, Florian Bemmann, Miriam Halsner, and Sven Mayer. 2023. A Mixed-Method Exploration into the Mobile Phone Rabbit Hole. *Proc. ACM Hum.-Comput. Interact.* 6, MHCI, Article 194 (sep 2023), 29 pages. https://doi.org/10.1145/3604241

[35] Yajin Zhou, Xinwen Zhang, Xuxian Jiang, and Vincent W Freeh. 2011. Taming information-stealing smartphone applications (on android). In *Trust and Trustworthy Computing: 4th International Conference, TRUST 2011, Pittsburgh, PA, USA, June 22-24, 2011. Proceedings 4*. Springer, 93–107.

[36] J Christopher Zimmer, Riza Arsal, Mohammad Al-Marzouq, Dewayne Moore, and Varun Grover. 2010. Knowing your customers: Using a reciprocal relationship to enhance voluntary information disclosure. *Decision Support Systems* 48, 2 (2010), 395–406. https://doi.org/10.1016/j.dss.2009.10.003