

The PIONEER Project: A PrIvacy companion for mOtivationN and knowlEdge transfER

Simon Althaus^{†‡}, Nina Gerber^{†‡}, Sara Hahn^{*†‡}, Andreas Heinemann^{*‡},
Angela Menig^{†‡}, Max Mühlhäuser^{†‡}, Christian Reuter^{†‡}, Ephraim Zimmer^{†‡}

[†] *Technical University of Darmstadt*

^{*} *University of Applied Sciences Darmstadt*

[‡] *ATHENE – National Research Center for Applied Cybersecurity*

Abstract

Remaining control over their private data is one of the key challenges in this century for users. We know from prior work that users are often neither in a position to fully grasp the content of the usually complicated texts, nor are they motivated to spend the time necessary to do so. We report on the progress made by the PIONEER project on a privacy support tool that combines knowledge transfer and persuasive elements to increase users' privacy awareness and motivation; thus empowering them to more privacy sovereignty. Throughout the research and design process, we consider user group specifics that may result in different requirements, e.g., for children, adolescents, parents, or elderly people. We further target sustainable behavior change by addressing different states of change, precisely: spark initial motivation, facilitate the creation of new habits, and encourage habituation of these habits in the long term (volition). Finally, we provide a privacy support tool demonstrator that can be utilized for research and education purposes, e.g., in school contexts.

1 Introduction

Remaining control over their private data is one of the key challenges in this century for users [1, 4, 13]. Attempts by legislators to help users meet this challenge such as the General Data Protection Regulation (GDPR) [5] in the EU are often based on the concept of “informed consent”. This assumes that users can decide according to their actual interest if they are provided with sufficient information, e.g., about how and by which actors their data will be processed. In practice, this is

reflected in extensive privacy statements or pop-up windows, e.g., informing about the use of cookies on various websites.

We know from prior work that users are often neither in a position to fully grasp the content of the usually complicated texts, nor are they motivated to spend the time necessary to do so [6–11, 14]. Hence, a new concept is required to ensure that users can make truly sovereign decisions about the handling of their data in everyday digital life, which (1) conveys the necessary knowledge, (2) strengthens the users' motivation to acquire competencies in this area and apply these in everyday digital life, especially taking into account (3) specifics that evolve from different user groups, like elderly people or adolescents.

We are thus striving for the user-centered as well as user group diacritic development of a digital privacy companion in the form of a mobile app that combines all three elements.

1. The app provides the necessary knowledge about digital contexts to enable users to actually make self-determined, informed decisions about how to handle their data.
2. We further apply psychological motivation theories to address psychological needs (e.g., autonomy, competence, relatedness) that drive human behavior but have sparsely been considered in the Usable Security and Privacy context so far. In addition, we build on the Persuasive System Design framework [12] to identify persuasive principles that support users to show and maintain privacy-aware behavior in the long term.
3. Our user-centered development explicitly examines and considers specifics of the aforementioned goals and methods that derive from different user groups, since, e.g., elderly people are driven by different psychological needs than younger generations, and children and adolescents need to be addressed with a different level of knowledge about digital contexts than adults.

We provide an overview of the research conducted by the PIONEER project in the remainder.

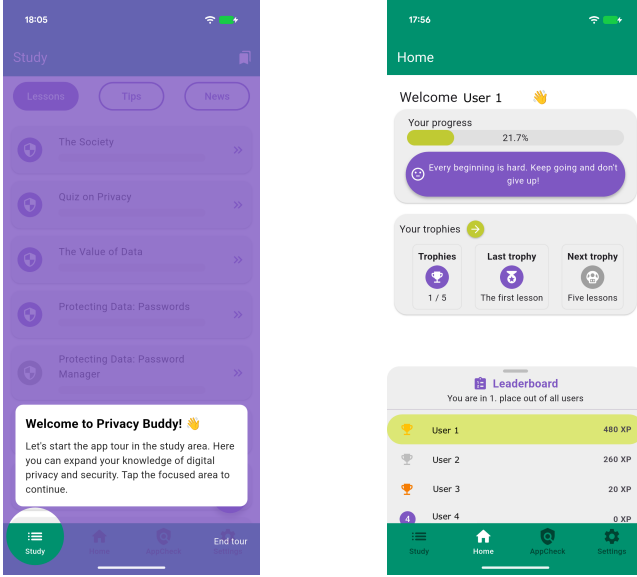


Figure 1: Screenshots of our privacy companion.

2 Current Investigations & Results

2.1 Technical Realization

We developed an initial prototype companion app for Android. We collected and reviewed relevant literature on the implementation of persuasive mechanisms as well as on the customization of mobile applications with respect to different user groups. Building on several iterations of usability evaluations, the prototype was improved through redesign efforts and the introduction of new features like multilingual support, cross-platform availability, survey integration, and a guided on-boarding experience. In addition, pipelines for machine learning-based features enable the analysis of privacy policies, chat bot support, and assistance for creation of teaching content. We further implemented a modular and extensible framework for mobile app analysis, which serves analysis results to the companion app about the privacy of mobile Android apps. In addition, research on Android’s Data Safety Section revealed fewer discrepancies than previously reported when applying refined definitions. Complementing this, new user analysis and Android tracing frameworks were designed and implemented [2, 3].

2.2 Persuasive Systems Design and User Groups

We conducted multiple studies to iteratively refine the companion app within a user-centered design process. These included (1) a design thinking study to analyze and derive persuasive app features based on psychological needs, (2) a controlled online experiment investigating visualizations of privacy policies, and (3) expert focus groups to identify relevant

privacy situations and data flows based on contextual integrity. Our key findings from the focus groups are that structuring privacy information, ensuring verifiability, and highlighting the credibility of providers is prioritized over gamification elements which seem unsuited in the privacy context. The online experiment showed that visual metaphors displaying which data flows towards third parties and which is stored only by the data collector facilitate understanding and are preferred by users. In addition, we focused on children and teenagers as specific user groups and conducted interviews to understand their privacy support needs and requirements. Based on these findings, we created a video directly addressing children and teens to support them in managing their privacy on social media. We also added lessons to the prototype based on privacy training materials validated in a previously conducted user survey study. Furthermore, we conducted a systematic literature review to identify the most promising persuasive mechanisms and their combinations, identifying primary task support as the most promising, followed by dialogue and social features.

2.3 Psychological Needs

Our ongoing research entails several empirical and design-oriented activities. (1) We conducted an interview study with young adults to examine their privacy-related decision-making and to investigate how these decisions relate to underlying psychological needs. We found that their key motivation, wanting to feel competent or entertained, or maintain close contact with friends, outweighed their privacy concerns. (2) We further performed usability evaluations of the current version of our app in order to assess user interaction and identify opportunities for improvement. (3) In addition, we held focus groups with both users and domain experts to explore perspectives on privacy decision-making in greater depth and confirmed the information type to be of great importance. We created a scenario set of daily privacy scenarios with varying types that will be used in a follow-up quantitative study. (4) We conducted co-creation workshops aimed at developing need-sensitive design approaches for trustworthy permission approval processes in smartphone analysis. The outcomes of these workshops inform iterative design improvements and were evaluated in a quantitative follow-up study investigating the relationship of need fulfillment and trust in our app. Such trust-building elements include an overview of apps accessing personal data, permission management options, a privacy score, and privacy certificates.

Acknowledgments

This research work was supported by the National Research Center for Applied Cybersecurity ATHENE. ATHENE is funded jointly by the German Federal Ministry of Research, Technology and Space and the Hessian Ministry of Science and Research, Arts and Culture.

References

- [1] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. Secrets and likes: the drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology*, 30(4):736–758, 2020.
- [2] Nikolaos Alexopoulos, Simon Althaus, and Diomidis Spinellis. Slicedroid: Towards reconstructing android application i/o behaviors from kernel traces, 2025.
- [3] Simon Althaus, Nikolaos Alexopoulos, Max Mühlhäuser, Christian Reuter, and Ephraim Zimmer. Wootdroid: Whole-system online on-device tracing for android, 2026.
- [4] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. Americans and privacy: Concerned, confused and feeling lack of control over their personal information, 2019.
- [5] European Commission. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), 2016.
- [6] Colin M. Gray, Cristiana Santos, Nataliia Bielova, Michael Toth, and Damian Clifford. Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.
- [7] Paul Graßl, Hanna Schraffenberger, Frederik Zuiderveen Borgesius, and Moniek Buijzen. Dark and bright patterns in cookie consent requests. *Journal of Digital Social Research*, 3(1):1–38, 2021.
- [8] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. "it's a scavenger hunt": Usability of websites' opt-out and data deletion choices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–12, New York, NY, USA, 2020. Association for Computing Machinery.
- [9] Dominique Machuletz and Rainer Böhme. Multiple purposes, multiple problems: A user study of consent dialogs after gdpr. *Proceedings on Privacy Enhancing Technologies*, 2020(2):481–498, 2020.
- [10] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. Dark patterns after the gdpr: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–13, New York, NY, USA, 2020. Association for Computing Machinery.
- [11] Jonathan A. Obar and Anne Oeldorf-Hirsch. The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 23(1):128–147, January 2020.
- [12] Harri Oinas-Kukkonen and Marja Harjumaa. Persuasive systems design key issues, process model, and system features. *Communications of the Association for Information Systems*, 24, 2009.
- [13] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. Awareness, adoption, and misconceptions of web privacy tools. *Proceedings on Privacy Enhancing Technologies*, 2021(3):308–333, 2021.
- [14] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. (un)informed consent: Studying gdpr consent notices in the field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, page 973–990, New York, NY, USA, 2019. Association for Computing Machinery.