# Designing and Evaluating Scalable Privacy Awareness and Control User Interfaces for Mixed Reality

MARVIN STRAUSS, Human-Computer Interaction Group, University of Duisburg-Essen, Germany
VIKTORIJA PANEVA, Usable Security and Privacy Group, University of the Bundeswehr Munich, Germany
FLORIAN ALT, Usable Security and Privacy Group, University of the Bundeswehr Munich, Germany
STEFAN SCHNEEGASS, Human-Computer Interaction Group, University of Duisburg-Essen, Germany

## 1 MOTIVATION

In the realm of Extended Reality (XR), Mixed Reality (MR) headsets represent a technological convergence, bridging Augmented Reality (AR) and Virtual Reality (VR) [7, 9]. These headsets offer an unprecedented level of immersion and interactivity, catering to a wide array of applications across various industries [6]. The versatility of MR headsets, ranging from entertainment to professional training, positions them as a pivotal component in the next wave of digital transformation. However, the rapid evolution of these technologies necessitates a proactive approach to address the emerging challenges they present, particularly in the domains of privacy, ethics, and user safety [2].

The escalating adoption of MR headsets brings to the fore significant privacy concerns [3]. These devices, by their very nature, are capable of capturing extensive data about users, their environment, and their surroundings [4]. This data, if misused, could lead to unsolicited profiling or surveillance, posing a threat to individual privacy and societal norms [10]. The potential for such misuse underscores the urgent need for policies that safeguard against these risks [1].

Key challenges in this domain include raising users' and bystanders' awareness and increasing their understanding of the privacy implications of XR technologies [5, 8]. Moreover, the investigation of their privacy perception towards these devices is important to understand their concerns and desires. Consequently, it is crucial to protect all parties from the unaware or unwanted collection of sensitive data. This protection must be balanced with the continued innovation and utility of XR technologies.

## 2 OPEN RESEARCH QUESTIONS

In the context of the challenges associated with increasing awareness of data collection and privacy implications on MR devices, the following open research questions emerge:

(1) How can MR user interfaces raise awareness among users about the data being collected, processed, and shared?
(2) How can users' MR privacy behavior be investigated in realistic settings?

Authors' addresses: Marvin Strauss, marvin.strauss@uni-due.de, Human-Computer Interaction Group, University of Duisburg-Essen, Essen, Germany; Viktorija Paneva, viktorija.paneva@unibw.de, Usable Security and Privacy Group, University of the Bundeswehr Munich, Munich, Germany; Florian Alt, florian.alt@unibw.de, Usable Security and Privacy Group, University of the Bundeswehr Munich, Munich, Germany; Stefan Schneegass, stefan.schneegass@uni-due.de, Human-Computer Interaction Group, University of Duisburg-Essen, Essen, Germany.


Manuscript submitted to ACM

(3) How can bystanders of MR users be informed of ongoing tracking and be granted control over their data?
(4) How can MR user interfaces efficiently communicate privacy risks associated with consenting to data collection and sharing at opportune moments?
(5) How can MR user interfaces support efficient privacy permission control, including understanding, granting, reviewing, and revoking permissions?
(6) How can the impact of MR privacy interfaces be assessed?
(7) How can researchers and practitioners be supported in the privacy-preserving design of MR applications?

## 3 RESEARCH ROADMAP

We sketch a research roadmap to address the aforementioned research questions. Firstly, a profound **understanding of users' awareness, mental models, and their understanding of the implications of using MR technology on their privacy** needs to be obtained. This knowledge is crucial for informing the design of privacy-preserving user interfaces in a way that raises users' awareness, supports users in building up the required proficiency, and gives users control and feedback mechanisms to make strong and informed decisions.

Secondly, **usable privacy control UIs for MR applications and devices** need to be created. As many privacy mechanisms are deliberately designed with low usability, that is, designers increase the interaction costs in terms of time and effort in a way that users ignore them or deliberately violate UI guidelines to bias users' decisions (cf. cookie banners, privacy policies, and permission systems). As a result, facilitating the design of user interfaces that (a) minimize the effort for users, and (b) enable strong and confident privacy decisions, scaling to the ever-increasing number of devices and applications becoming available for MR, is key.

Thirdly, the developed **privacy control UIs need to be evaluated**. On one hand, there is a need to rigorously measure the usability of the concepts, quantifying how easy they are to learn, how efficiently they can be used, how easy they make it for users to memorize privacy decisions, and how satisfied users are. On the other hand, an interesting question is how concepts affect privacy behavior for other technologies, how users' self-efficacy evolves, and how interfaces can be designed not to make users dependent.

Finally, a core challenge in evaluating privacy user interfaces regarding long-term effects is creating an environment in which users behave naturally and in an unbiased way. A **real-world testbed** is required where privacy user interfaces can be evaluated in users' everyday lives as they interact with MR technology.

By fulfilling these objectives, it becomes possible to embed privacy as an integral aspect of the design of MR applications and provide a valuable resource for researchers, practitioners, and manufacturers that empowers them to address privacy challenges during the design and development phases rather than as an afterthought.

## 4 CONCLUSION

To conclude, the widespread adoption of XR technologies, particularly MR, presents opportunities and challenges. As we stand at the cusp of this technological revolution, it is crucial to develop policy frameworks that not only encourage responsible innovation but also address potential vulnerabilities. With our research, we aim to take a proactive step in this direction, aiming to integrate privacy considerations into the fabric of MR and XR technology design and development. By participating in this workshop, we aim to contribute to the collaborative effort of charting a responsible and sustainable course for the XR landscape, ensuring that innovation does not come at the cost of privacy and ethical considerations.

## REFERENCES


[1] Devon Adams, Alseny Bah, Catherine Barwulor, Nureli Musaby, Kadeem Pitkin, and Elissa M. Redmiles. 2018. Ethics Emerging: the Story of Privacy and Security Perceptions in Virtual Reality. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, 427–442. https://www.usenix.org/conference/soups2018/presentation/adams

[2] Kent Bye, Diane Hosfelt, Sam Chase, Matt Miesnieks, and Taylor Beck. 2019. The ethical and privacy implications of mixed reality. In *ACM SIGGRAPH 2019 Panels*. 1–2.

[3] Jaybie A De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. 2023. Privacy and Security Issues and Solutions for Mixed Reality Applications. In *Springer Handbook of Augmented Reality*. Springer, 157–183.

[4] Vivek Nair, Gonzalo Munilla Garrido, and Dawn Song. 2023. Exploring the Unprecedented Privacy Risks of the Metaverse. https://doi.org/10.48550/arXiv.2207.13176 arXiv:2207.13176 [cs].

[5] Joseph O'Hagan, Pejman Saeghe, Jan Gugenheimer, Daniel Medeiros, Karola Marky, Mohamed Khamis, and Mark McGill. 2023. Privacy-Enhancing Technology and Everyday Augmented Reality: Understanding Bystanders' Varying Needs for Awareness and Consent. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 6, 4 (Jan. 2023), 177:1–177:35. https://doi.org/10.1145/3569501

[6] Sang-Min Park and Young-Gab Kim. 2022. A metaverse: Taxonomy, components, applications, and open challenges. *IEEE access* 10 (2022), 4209–4251.

[7] Philipp A. Rauschnabel, Reto Felix, Chris Hinsch, Hamza Shahab, and Florian Alt. 2022. What is XR? Towards a Framework for Augmented and Virtual Reality. *Computers in Human Behavior* 133 (2022), 107289. https://doi.org/10.1016/j.chb.2022.107289

[8] Philipp A. Rauschnabel, Jun He, and Young K. Ro. 2018. Antecedents to the adoption of augmented reality smart glasses: A closer look at privacy risks. *Journal of Business Research* 92 (Nov. 2018), 374–384. https://doi.org/10.1016/j.jbusres.2018.08.008

[9] Maximilian Speicher, Brian D. Hall, and Michael Nebeling. 2019. What is Mixed Reality?. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3290605.3300767

[10] P.P. Tricomi, F. Nenna, L. Pajola, M. Conti, and L. Gamberi. 2023. You Can't Hide Behind Your Headset: User Profiling in Augmented and Virtual Reality. *IEEE Access* 11 (2023), 9859–9875. https://doi.org/10.1109/ACCESS.2023.3240071