Department: Security and Privacy
Editor: Florian Alt, florian.alt@unibw.de

Privacy in the Metaverse

About the Need for Privacy-Preserving Technologies in XR

Viktorija Paneva
University of the Bundeswehr, Munich

Marvin Strauss
University of Duisburg-Essen

Verena Winterhalter
University of the Bundeswehr, Munich

Stefan Schneegass
University of Duisburg-Essen

Florian Alt
University of the Bundeswehr, Munich

■ **DISCUSSIONS ON THE "METAVERSE"** today more often than not home in on the question of *when* this vision is going to become a reality – rather than questioning *whether* this will ever happen. In addition, there is agreement among experts that head-mounted XR displays will become the main pervasive technology enabling participation in the metaverse. The recent excitement about the metaverse primarily stems from its economic potential, and it is evident that, like in the Internet, user data will be a core currency.

We take the stance that it is essential to start thinking about how users' data can be protected in the metaverse. To this end, we reflect on how the metaverse future might look if we do not take action, drawing parallels to the development of the Internet. We then briefly point towards ongoing activities before outlining research challenges to be addressed to make privacy protection one of the primary design goals for devices, services, and apps in the metaverse. Finally, we sketch a privacy-focused research roadmap.

When Will the Metaverse Become a Reality?

Despite its presence in the media, it remains somewhat unclear when we will see the first examples of the metaverse as envisioned by practitioners and researchers. Currently, the technical infrastructure, bandwidth, and lack of appropriate interaction techniques are among the main challenges that need to be addressed before the metaverse vision can become a reality.

Experts seem to agree that the anticipated profit will be the driving force behind the evolution of the metaverse, similar to what we saw happening with the traditional Internet. The ability to reach customers around the globe at any time means unveiling their interests, behavior, and even political and religious views by analyzing their click stream, as well as easily reaching their social circle by analyzing the user's social network. This led to an unanticipated evolution of the Internet, and one important challenge: privacy.

Why is Privacy a Challenge for the Metaverse?

During the design and evolution of novel, pervasive technologies, privacy often takes a back seat. Designers and developers are typically more focused on exploring the exciting new possibilities that emerge with these technologies in terms of innovative features, rather than investing time in considering privacy and security implications. Privacy is often treated as an issue that can be solved later. For example, in 2018, Oculus stated secure communication encryption is not a priority as it is likely to introduce latency and negatively affect user experience. Meanwhile, threats evolve over time and might not be fully foreseeable during the creation of technology. Consequently, there has been increasing attention from the research community on the importance of privacy-preserving methods in XR environments [1].

Protecting privacy in the metaverse presents significant challenges. The collected data cannot only be used to facilitate interaction but also enable the inference of sensitive user information. This can potentially invade users' privacy, allowing third parties to obtain information that users might not realize they shared. For example, telemetry and eye gaze data can be used to infer information on users' well-being, literacy, and vision impairments [2], their political views and gender [3], and even their identity [4], [5].

Addressing privacy concerns after the system is built has a long tradition in computer science. For instance, years after the implementation of cookies, legislators introduced mandatory cookie banners to mitigate their privacy implications for the general public. However, while this approach enables users to make informed decisions in theory, it often falls short in practice due to the use of deceptive designs and the cognitive effort required to comprehend the information provided. To avoid implementing privacy measures post hoc, we argue for the need to research and develop such measures in the design phase.

Why Should We Care Now?

User data has quickly become a core currency of the Internet. Websites track users across platforms, using this data to infer information such as gender, age, interests, political views, and sexual orientation, among others, to tailor content more effectively. Meanwhile, insurance companies and other entities use insights into users' behavior to offer a range of services. Only very slowly do people begin to realize the implications of this and the need for action.

The data protection movement is still in its early stages, with the GDPR (General Data Protection Regulation) as a prominent example of an initial attempt to empower individuals with control over their data. While being a step in the right direction, the GDPR and the call for privacy by design have not accomplished the desired effect. Instead, they led to practices that make achieving the objectives even more challenging: setting privacy permissions does not scale, leading users to quickly give up on the idea of being able to manage which sensors (and data) each app and service they use should have access to [6]. Furthermore, consent mechanisms are often useless, as information on what data a device or service can access, collect, process, and share is buried deep within End User License Agreements (EULAs) and privacy statements, vastly exceeding the effort users are willing to invest in order to fully understand what they consent to.

Looking ahead, the integration of sensors into XR technologies brings data collection even closer to the user's physical body, heightening privacy concerns. Taking action now is crucial to seize any remaining opportunity to safeguard our data in the metaverse.

How Do We Protect Privacy in the Metaverse?

In the following, we outline several research challenges that need addressing in the future to avoid the privacy pitfalls observed on the web from simply rolling over as the vision of the metaverse evolves in the years to come. By all means, we must avoid a future where users are left only with the choice between exposing an ever-increasing amount of sensitive data or opting out of participating in the digital transformation.

Stakeholders

Realizing a privacy-preserving approach to XR requires a focus on various stakeholders. *Designers* and *developers* need to be provided with clear guidance to ensure that services and applications for the metaverse are created with privacy in mind. Currently, design patterns and guidelines, such as Shneiderman's Eight Golden Rules for user interface design [7], are largely missing when it comes to usable privacy. A first step towards such guidance is the code of ethics developed by Adams et al. [1], which advocates for the use of secure protocols, transparency in data collection practices, and obtaining user permission each time data is collected. However, practical guidance on how to implement these principles in practice is still lacking today.

The second stakeholder group are *end users*, encompassing both device owners and users, as well as bystanders who may be affected, for example, by being in the field of view of an HMD's outward-facing camera. User interfaces should be designed to support all user groups in interacting with the metaverse in a privacy-preserving way.

Administrators and *legislators* also play an important role in shaping the emerging privacy landscape of the metaverse. Effective regulations should adapt to the unique challenges posed by XR technologies, such as pervasive data collection through integrated sensors.

Through participatory design efforts involving all relevant stakeholders—from designers and developers to end users, administrators, and legislators—we can collectively shape a metaverse that respects user privacy while fostering innovation and digital engagement.

End-User Perspective

Users currently lack awareness, proficiency, and trust as they are required to engage with privacy in XR. This is largely a result of users' motivation but also of learned helplessness, as users realized that behaving in a privacy-preserving way is close to impossible.

Awareness and Proficiency A major challenge at the moment is that users of XR devices generally lack knowledge of which data HMDs are able to collect about them. Recent research highlights that users often have limited awareness of the granular data collection capabilities of XR sensors, such as their ability to capture involuntary body signals indicative of emotional responses [8]. Additionally, users are uncertain about who may have access to their data, and the possible implications. For instance, with an HMD equipped with an eye tracker, users are typically unaware that access to this data allows not only the gaze point to be inferred but also provides insights into the user state, demographics, and identity [3]. Hence, there is a clear need to better understand users' mental models and how we can support them in understanding what it means to use HMDs equipped with sensors.

Furthermore, users generally do not know when and which data is collected. This lack of awareness poses a challenge not only for the main user but also for bystanders. This is comparable to situations today, in which bystanders may appear in photos posted on social media without their knowledge. As XR technology becomes more pervasive, this challenge will intensify if suitable measures are not taken to address these concerns.

Efforts are required to improve user understanding of how their interactions with XR devices affect their privacy and enhance proficiency and autonomy in navigating privacy settings.

Trust Closely related to awareness and proficiency is trust in the data collection practices in the metaverse. This can be compared to concerns about whether a user can be sure that Alexa's microphone is not recording when the respective button is pressed, indicated by a red light. This lack of trust often leads users to physically unplug a device or deploy means to disable the functionality of a sensor, such as placing a physical cover over a smartphone or laptop's camera.

Furthermore, there is the question of whether a device or service provider really uses the data only in the way that was communicated to the user. Today, privacy boxes can control incoming and outgoing traffic of a (home) network, ensuring that only data explicitly consented to by the user is transmitted. However, similar to privacy permissions, the effort required for configuration and the technical expertise usually necessary for setup make these approaches still difficult for many people to use.

Building trust in XR technologies requires transparent data practices and user-friendly privacy controls. Enhancing user understanding and providing simple tools for managing privacy are essential for fostering users' trust in a privacy-protecting metaverse experience.

User Interfaces

As mentioned above, user interfaces are often designed to make it as difficult as possible for users to protect their privacy. Novel approaches are required to support the users in making quick and confident privacy decisions.

Feedback Firstly, feedback mechanisms are needed to make it instantly apparent to users and bystanders which data is being collected. An example today is the LED indicating an activated camera. However, such mechanisms would have to be extended and reevaluated for XR technologies, ensuring clarity and transparency in the type and extent of data collection in relation to the different sensors and stakeholders.

Control There is a need for mechanisms that give users the ultimate control of what happens to their data. Current mechanisms, like privacy permissions, do not scale well as users have to set hundreds of permissions for the many services and devices they use. Possible approaches could abstract from this complexity; for example, by allowing users to specify types of data and contexts in which they would be comfortable with data collection, streamlining privacy management efforts. For instance, Delgado et al. [9] presented an approach for smart home privacy that, through tangible interaction, allows all sensors of a particular type (e.g., camera, microphone) to be activated or deactivated in a specific context. This kind of approach could not only simplify user interaction but also make user control over their privacy preferences in dynamic environments like the metaverse more accessible and effective.

Methodology

Next, we explore methodological challenges in addressing privacy in XR, focusing on devising effective privacy metrics and adopting appropriate research approaches.

Privacy Metrics Privacy is difficult to quantify and thus needs to be carefully considered in research to avoid issues similar to those encountered with cookie banners. Establishing robust metrics for privacy in XR environments is crucial for measuring the efficacy of privacy protection mechanisms and upholding privacy standards. Potential metrics could encompass aspects such as data minimization, user consent practices, transparency of data usage, and resilience against potential privacy breaches. Moreover, it is important for the metric to evolve with the technology, and user requirements and expectations, to ensure ongoing relevance and effectiveness in safeguarding user privacy in XR.

Research Approach Addressing the challenge of investigating privacy-related phenomena in XR environments, and in general, involves navigating the privacy paradox. This paradox reflects the discrepancy where individuals express a desire to protect their (online) privacy but often behave in ways that contradict this intention. Therefore, evaluating novel privacy control interfaces for XR requires diverse research approaches, ranging from controlled experiments to quantify usability aspects to long term field experiments that capture actual changes in behavior, proficiency, and self-efficacy. Transitioning research into real-world settings is crucial for overcoming the limitations of controlled environments and gaining practical insights into user behavior. Despite the complexities and logistical challenges associated with field studies, they provide an unmatched opportunity to assess the practical efficacy of privacy solutions and gather authentic user feedback. By combining controlled lab studies with real-world testbeds, researchers can ensure that privacy solutions for XR are technically sound, effective, and user-centric.

Open Research Questions

In the context of the challenges associated with increasing awareness of data collection and privacy implications of XR devices in the metaverse, the following research questions emerge:

- How can XR user interfaces effectively raise awareness among users about the data being collected, processed, and shared?

- How can users' privacy behavior be investigated in realistic day-to-day user engagements within the metaverse?
- How can bystanders of users with XR devices be informed about ongoing tracking and be granted control over their data?
- How can user interfaces in the metaverse efficiently communicate privacy risks associated with consenting to data collection and sharing, at opportune moments?
- How can user interfaces in the metaverse support efficient privacy permission control, including understanding, granting, reviewing, and revoking permissions?
- How can the effectiveness of privacy protection mechanisms and interventions for XR devices be reliably measured and evaluated?
- How can designers and other practitioners be effectively supported in implementing privacy-preserving design practices for XR apps?

Research Roadmap

We outline 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 XR 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 XR applications and devices** need to be created. As many privacy mechanisms are deliberately designed with low usability – where 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) – 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 in the metaverse, 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. A core challenge in evaluating privacy user interfaces regarding long-term effects is creating an environment in which users behave naturally and unbiasedly. A **real-world testbed** is required where privacy user interfaces can be evaluated in users' everyday lives as they interact with XR.

By fulfilling these objectives, it becomes possible to embed privacy as an integral aspect of the design of metaverse 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.

Conclusion

In this article, we highlight the urgent need to integrate privacy considerations into the fabric of XR technology design and development. The widespread adoption of XR technologies presents both 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. By focusing on privacy-preserving technologies from the outset, we can ensure that the metaverse evolves into a space where users' data is respected, their autonomy is upheld, and trust in digital interactions is reinforced. This proactive approach will be essential in shaping a metaverse that not only thrives economically but also prioritizes the fundamental rights and freedoms of its users.

ACKNOWLEDGMENT

This work has received funding from the German Research Foundation (DFG) under grant agreement no. 521584224.

REFERENCES

1. D. Adams, A. Bah, C. Barwulor, N. Musaby, K. Pitkin, and E. M. Redmiles, "Ethics emerging: the story of privacy

and security perceptions in virtual reality," in *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 427–442. [Online]. Available: https://www.usenix.org/conference/soups2018/presentation/adams

2. V. Nair, G. M. Garrido, D. Song, and J. O'Brien, "Exploring the privacy risks of adversarial vr game design," *Proceedings on Privacy Enhancing Technologies*, 2023.
3. J. Steil, I. Hagestedt, M. X. Huang, and A. Bulling, "Privacy-aware eye tracking using differential privacy," in *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications*, ser. ETRA '19. New York, NY, USA: Association for Computing Machinery, 2019. [Online]. Available: https://doi.org/10.1145/3314111.3319915
4. K. Pfeuffer, M. J. Geiger, S. Prange, L. Mecke, D. Buschek, and F. Alt, "Behavioural biometrics in vr: Identifying people from body motion and relations in virtual reality," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, ser. CHI '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 1–12. [Online]. Available: https://doi.org/10.1145/3290605.3300340
5. J. Liebers, M. Abdelaziz, L. Mecke, A. Saad, J. Auda, U. Gruenefeld, F. Alt, and S. Schneegass, "Understanding user identification in virtual reality through behavioral biometrics and the effect of body normalization," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, ser. CHI '21. New York, NY, USA: Association for Computing Machinery, 2021. [Online]. Available: https://doi.org/10.1145/3411764.3445528
6. S. Prange, P. Knierim, G. Knoll, F. Dietz, A. D. Luca, and F. Alt, "I do (not) need that feature! – understanding users' awareness and control of privacy permissions on android smartphones," in *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. Philadelphia, PA: USENIX Association, Aug. 2024. [Online]. Available: https://www.usenix.net/conference/soups2024/presentation/prange
7. B. Shneiderman, C. Plaisant, M. S. Cohen, S. Jacobs, N. Elmqvist, and N. Diakopoulos, *Designing the user interface: strategies for effective human-computer interaction*. Pearson, 2016.
8. H. Hadan, D. M. Wang, L. E. Nacke, and L. Zhang-Kennedy, "Privacy in immersive extended reality: Exploring user perceptions, concerns, and coping strategies," in *Proceedings of the CHI Conference on Human Factors in Computing Systems*, ser. CHI '24. New York, NY, USA: Association for Computing Machinery, 2024. [Online]. Available: https://doi.org/10.1145/3613904.3642104
9. S. Delgado Rodriguez, S. Prange, C. Vergara Ossenberg, M. Henkel, F. Alt, and K. Marky, "Prikey – investigating tangible privacy control for smart home inhabitants and visitors," in *Nordic Human-Computer Interaction Conference*, ser. NordiCHI '22. New York, NY, USA: Association for Computing Machinery, 2022. [Online]. Available: https://doi.org/10.1145/3546155.3546640

Viktorija Paneva is a postdoctoral researcher at the CODE Research Institute for Cyber Defense at the University of the Bundeswehr in Munich, Germany. She is the corresponding author of this article. Contact her at vpaneva@acm.org

Marvin Strauß is a doctoral researcher at the University of Duisburg-Essen, Germany. Contact him at marvin.strauss@uni-due.de

Verena Winterhalter is a doctoral researcher at the CODE Research Institute for Cyber Defense at the University of the Bundeswehr in Munich, Germany. Contact her at verena.winterhalter@unibw.de

Stefan Schneegass is a Full Professor of Computer Science at the University of Duisburg-Essen, Germany. Contact him at stefan.schneegass@uni-due.de

Florian Alt is a Full Professor of Usable Security and Privacy at the CODE Research Institute for Cyber Defense at the University of the Bundeswehr in Munich, Germany. Contact him at florian.alt@unibw.de