Enhancing User Engagement with Game-Inspired Privacy Interfaces in Virtual Reality

Verena Winterhalter
LMU Munich, Germany
verena.winterhalter@ifi.lmu.de

Viktorija Paneva
LMU Munich, Germany
viktorija.paneva@ifi.lmu.de

Florian Alt
LMU Munich, Germany
University of the Bundeswehr, Germany
florian.alt@ifi.lmu.de

Abstract

Virtual reality (VR) applications collect extensive user data, often without users' full awareness. Current privacy interfaces in VR are frequently adapted from 2D systems and fail to leverage the immersive, spatial nature of VR. In this work, we explore how game elements can be used to design more engaging and effective privacy interactions in VR. Using a VR escape room environment, we conducted in-VR sketching sessions with novice game designers (n=12). Participants developed 17 privacy interaction concepts, 4 of which are highlighted in this poster for their creative use of game mechanics and metaphors. Our findings suggest that integrating privacy interactions into the game environment can raise user awareness and interest, but also highlight risks—such as blurring the line between gameplay and real privacy choices. We discuss these tensions and propose directions for refining and evaluating gamified privacy interfaces in VR.

1 Introduction and Background

VR headsets and other head-mounted displays collect a wide range of sensor data, often beyond what users are consciously aware of [3,4,7]. While much of this data supports interaction within virtual environments, it can also be used to infer personal information about the user and their surroundings [7]. This raises important privacy concerns, particularly in VR games and applications that are designed to be engaging and highly interactive [5].

At the same time, current privacy interfaces in VR often replicate 2D paradigms, missing the opportunity to leverage the spatial and interactive nature of immersive environments [8, 11]. As a result, these interfaces may struggle to meaningfully inform users or foster engagement with privacy-related decisions. Designing VR-native privacy interfaces offers a chance not only to address these limitations but also to turn privacy interactions into an integrated and compelling part of the user experience [1, 9].

Using gamification to increase user engagement has already been used in other fields [10, 12]. Ebbers et al. [2] found that users preferred the playful design of privacy features in a digital assistant. Lim et al. [6] used gamification to implement a privacy tutorial in VR.

In our work, we investigate how game elements can support the design of privacy interactions in VR. Our goal is to better understand how such elements can be used to raise awareness, increase user engagement, and foster more meaningful interaction with privacy settings and implications. This leads us to the following research question:

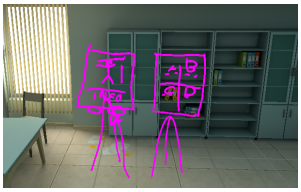
RQ: How can game elements be used in VR privacy interactions to increase user awareness and engagement?

2 Methodology

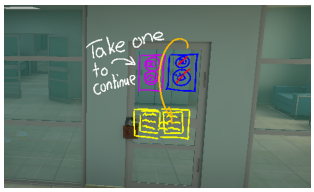
We used the VR escape room by Nair et al. [7] as our study environment. The escape room was specifically created to collect data and infer information about the player, so it is a suitable setting to illustrate the privacy challenge in VR. We selected four rooms from the office-building themed escape room for our study that collect different information about players while they try to solve the puzzle within the room:

- **Wingspan:** The puzzle is solved by striking certain body poses, allowing the system to calculate height and wingspan of the player.
- **Reaction time:** The puzzle requires quickly reacting to the color change of an object, which allows measuring the player's reaction time.
- **Color blindness:** The room has two possible solutions, one of which is only visible for players without red-green colorblindness.
- **Foreign language knowledge:** By analyzing eye track-

USENIX Symposium on Usable Privacy and Security (SOUPS) 2025.
August 10–12, 2025, Seattle, WA, United States.



(a) Whiteboard



(b) Privacy book

Figure 1: Design sketches from the VR sketching sessions.

ing data from the player looking at a wall with words in different languages, it can be inferred which languages the user is familiar with.

We held in-VR sketching sessions with novice game designers (n=12). We introduced them to the escape room [7] and explained how the rooms can be used to collect player data. We then asked the participants to brainstorm designs (individually or in small groups) and sketch one of them in VR, using a think-aloud protocol to explain their process. We then conducted semi-structured interviews to clarify design details, explore challenges, and discuss privacy considerations in game development.

We recorded and transcribed all sessions. Two researchers independently coded the data and collaboratively developed a shared codebook. We analyzed the codes to identify overarching themes. The study was approved by the ethics committee of the university where the study was conducted.

3 Results

A total of 17 ideas were described by the participants. We highlight four designs that make use of game design elements and gamification:

Design 1: Instead of mimicking body postures themselves, players can manipulate a mannequin with movable limbs to strike the poses. This offers an alternative game mechanism, allowing progress without tracking the player's wingspan. Another group proposed a similar idea with a separate mannequin for each pose.

Design 2: The player has a privacy companion, such as a small robot, who follows them around, offering information and guidance on privacy settings or questions. This interactive game character aims to increase user engagement by integrating into the application's context.

Design 3: Players make their privacy decisions by interacting with a computer and printer in the escape room, then sending their printed choice through pneumatic tubes for confirmation. The design uses elements that are already in the game setting to incorporate the privacy interface in a seamless way. Similarly, a second design uses a whiteboard and erasers as tools for the player to make their privacy decision (see Fig. 1a)

Design 4: Players document their privacy choices using stickers in a virtual book that they carry and can use anytime to modify their previous choices. The design uses a game metaphor (inventory) to make the privacy mechanism more accessible through a familiar concept (see Fig. 1b).

4 Discussion

We identified various game-related elements that serve different purposes regarding user privacy. Elements like the privacy companion or other in-game characters function as a *source of information* to provide the user with privacy information in an interactive, engaging way. Alternative game mechanics like the mannequins can help to *share less data* in the first place while still allowing the user to play the game. To achieve a *seamless integration* and *avoid disruption* from the gameplay, the designs explored the use of game elements adapted to the specific game setting (i.e., office setting of the escape room). Designs can also *apply familiar concepts* to make the privacy interfaces easy to use, such as the game metaphor of an inventory used for the privacy book.

Similar to related work in other fields [10, 12], we expect that incorporating game design elements into privacy interfaces could make privacy interactions more engaging for users, in turn raising interest in privacy and fuel the users' intrinsic motivation to engage with privacy decisions.

However, careful design is needed to avoid blurring the line between gameplay and real privacy choices. Additionally, using game objects to represent certain permissions or sensors may become difficult to scale as data types and sensors increase, potentially leading to repetitive, lengthy interactions.

5 Conclusion and Future Work

Using game elements in privacy interfaces can enhance user awareness and engagement by seamlessly integrating interfaces and applying familiar game concepts that provide information to the user. They can also help in protecting privacy by making use of alternative game mechanics that share less user data. Future work should further investigate how gamification can increase engagement and which game elements are most suitable for this. To contribute to this, we plan to refine and implement the designs, and evaluate them with users.

Presenting this work at SOUPS allows attendees to directly engage with the design concepts and reflect on the role of embodiment and interaction in privacy decision-making. It also creates space for dialogue between researchers and practitioners on how gamification and spatial design can shape more intuitive and meaningful privacy experiences as well as discuss future research directions.

Acknowledgments

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

References

[1] Jaybie A De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. Security and privacy approaches in mixed reality: A literature survey. *ACM Computing Surveys (CSUR)*, 52(6):1–37, 2019.

[2] Frank Ebbers, Jan Zibuschka, Christian Zimmermann, and Oliver Hinz. User preferences for privacy features in digital assistants. *Electronic Markets*, 31:411–426, 2021.

[3] Gonzalo Munilla Garrido, Vivek Nair, and Dawn Song. Sok: Data privacy in virtual reality. *arXiv preprint arXiv:2301.05940*, 2023.

[4] Hilda Hadan, Derrick M Wang, Lennart E Nacke, and Leah Zhang-Kennedy. Privacy in immersive extended reality: Exploring user perceptions, concerns, and coping strategies. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, pages 1–24, 2024.

[5] Jacob Leon Kröger, Philip Raschke, Jessica Percy Campbell, and Stefan Ullrich. Surveilling the gamers: Privacy impacts of the video game industry. *Entertainment Computing*, 44:100537, 2023.

[6] Junsu Lim, Hyeonggeun Yun, Auejin Ham, and Sunjun Kim. Mine yourself!: A role-playing privacy tutorial in virtual reality environment. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, pages 1–7, 2022.

[7] Vivek Nair, Gonzalo Munilla Garrido, Dawn Song, and James O'Brien. Exploring the privacy risks of adversarial vr game design. *Proceedings on Privacy Enhancing Technologies*, 2023.

[8] 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, 2020.

[9] Viktorija Paneva, Marvin Strauss, Verena Winterhalter, Stefan Schneegass, and Florian Alt. Privacy in the metaverse:. *IEEE Pervasive Computing*, 23(3):73–78, 2024.

[10] Daniele Ruggiu, Vincent Blok, Christopher Coenen, Christos Kalloniatis, Angeliki Kitsiou, Aikaterini-Georgia Mavroeidi, Simone Milani, and Andrea Sitzia. Responsible innovation at work: gamification, public engagement, and privacy by design. *Journal of Responsible Innovation*, 9(3):315–343, 2022.

[11] Florian Schaub, Rebecca Balebako, and Lorrie Faith Cranor. Designing effective privacy notices and controls. *IEEE Internet Computing*, 21(3):70–77, 2017.

[12] Ayoung Suh, Christian Wagner, and Lili Liu. Enhancing user engagement through gamification. *Journal of Computer Information Systems*, 58(3):204–213, 2018.