Understanding user awareness and attitudes towards attribute inferences from VR movement data

Camille Sivelle Ibrahim El Shemy Katrien De Moor
Norwegian University of Science and Technology

Abstract

Virtual Reality (VR) devices collect motion data for their core function, but this data has been shown to be prone to risks of re-identification and profiling through attribute inference. Prior work on VR privacy attitudes has found that users tend to accept motion data collection but express no awareness of these inference risks, making it unclear whether these findings reflect genuine comfort or simply a lack of information. This work-in-progress study addresses this gap through a Wizard-of-Oz lab experiment in which participants interact with a VR application that infers personal attributes from their motion data. By comparing the participants' awareness and privacy attitudes before and after the intervention, we aim to understand how increased awareness of motion data risks shapes users' attitudes towards its collection. In this poster, we present the design of the study and report on preliminary insights from an exploratory pilot with 4 participants.

1 Introduction

Virtual Reality (VR) is increasingly adopted, not only in entertainment but also in other domains such as education, healthcare and workplaces [3]. Despite the many opportunities this creates, the use of VR in other sectors also introduces various challenges that need to be addressed. Notably, the large volume of sensor data that VR systems continuously collect and process (e.g., motion, cameras, voice) raises novel privacy concerns [5, 7].

In particular, VR head-mounted displays (HMDs) rely on the constant collection of movement data (specifically, the positions and rotations of the headset and controllers) to situate the user in the virtual space. Previous studies demonstrated that this type of data contains sensitive patterns, which can be exploited not only to re-identify users across sessions [9, 10], but also to infer a range of personal attributes, including gender, age, ethnicity, physical characteristics, and behavioural traits [11–13], thus undermining users' privacy considerably.

However, in order to design privacy defences that are effective and meet users' needs, it is critical to understand how users perceive such risks and what protections they consider necessary. In this respect, prior studies found that VR users tend not to perceive movement data as sensitive [14], and consider its processing more acceptable than other data types, such as eye-tracking or camera data [6]. However, they also highlight that users may have a low awareness of the sensitive nature of VR data [6, 8, 14], which could be the main reason for this relative acceptance: current attitudes might be driven by a limited understanding of what this data can reveal, rather than an informed judgement.

Further research is needed to better understand the attitudes of VR users towards the collection of motion data and the potential need for protections, in particular whether these attitudes hold once users are made aware of the broader implications of this data collection.. A key question is therefore: *What (informed) privacy concerns do VR users express when made aware, via real-time inference demonstrations, of what their VR motion data reveals, and how do these differ from their initial concerns?* In this work-in-progress, we conduct an exploratory lab study in which participants interact with a VR application that attempts to predict several of their socio-demographic, physical and behavioural attributes. This poster reports on the design of the study, as well as on early insights from a pilot conducted with 4 participants.

2 Research approach

Our approach consists in exposing users to a VR app that pretends to infer attributes and shows predictions to the user, with the aim of providing a more experiential and visceral

USENIX Symposium on Usable Privacy and Security (SOUPS) 2026.
August 23–26, 2026, Hannover, Germany.

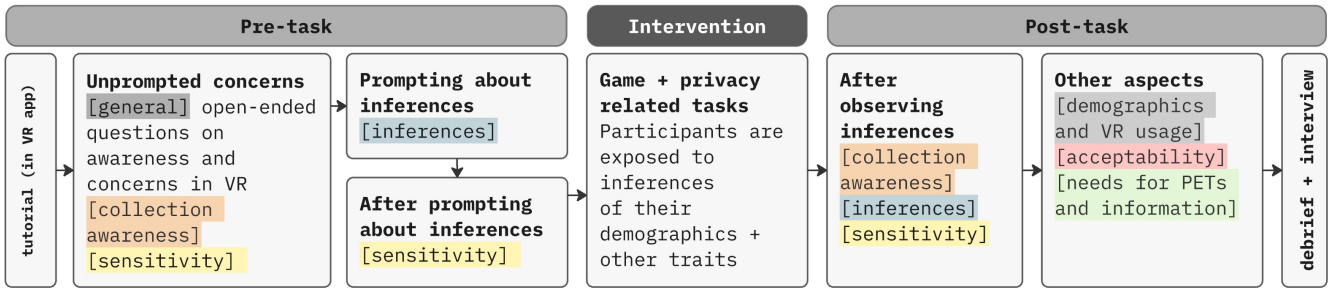

Figure 1: Overview of process followed in the pilot. We use questionnaires to measure the participants' privacy perceptions and awareness of inferences before and after exposing them to a VR application that attempts to make such inferences about them.

understanding of inferences from motion data. The goal is not to create long-term behavioural change, but rather to elicit informed concerns and inform the design of future privacy mechanisms. In other contexts than VR, prior studies have used similar approaches to confront users to secondary inferences in order to probe privacy attitudes and awareness [2, 4].

We adopt a pre/post-test within-subjects design (see Figure 1), based on a questionnaire that features repeated blocks of questions evaluating awareness and concerns, before and after our intervention. The goal of this design is to (1) validate whether the application increased the participants' awareness of the potential risks associated with the large-scale collection of VR motion data, and (2) explore the participant's attitudes and concerns towards the collection of VR motion data, when informed about these risks.

The application · The application used consists of a mini-game structured over three levels, adapted from [1]. The participant shoots targets that move at a speed which increases at each level. Between each of the levels, a pop-up prompts a privacy-related task requiring the participant to open and interact with a "privacy centre" which notably contains a panel where the participant can see a profile with all the inferences that the system made about them. This "inference view" is visible during the first two tasks but interaction with it is not required, while the third task explicitly directs participants to it, to ensure that all participants interact with it at least once.

In this Wizard-of-Oz setup, the value for each inference is set in real time by an experimenter when the participant wears the headset. While some of the traits are reliably observable, others require the experimenter to make a guess and may lead to inaccurate inferences — however, it remains realistic for such inferences to not always be totally accurate [12].

Deception and ethics · The study employs a semi-covert design: we do not initially mention our focus on inferences in order not to prime participants and to capture more authentic reactions, but they are told right before the intervention that the focus of the study is on evaluating the "privacy centre" interface, which also provides a plausible motivation for the navigation tasks through which participants first encounter the inference panel. Participants are fully debriefed after completing the post-task questionnaires. In addition, we do not collect or store any of the data related to the inferences themselves. The study design and data collection process were approved by the Norwegian Data Protection Authority.

Measurements · We measure the perceived sensitivity, data collection awareness, and inference awareness, using questions inspired from previous studies on privacy perceptions in VR (e.g., [6, 8, 14]). We repeat each block at multiple points throughout the study (as illustrated in Figure 1) to be able to draw comparisons before and after the intervention. In addition, sensitivity questions are also repeated after participants are prompted to consider potential inferences, allowing us to examine intra-questionnaire effects (for instance, whether thinking about inferences already leads participants to retroactively rate certain data types as more sensitive).

3 Early insights and expected contribution

We pilot tested the application, procedure and instruments with 4 university employees. Based on feedback from these pilot sessions, we made several adjustments, notably to more actively direct participants' attention toward the inferences being made. The study itself is currently in the data collection phase (n=25), and early insights tend to confirm the hypothesized lack of awareness of inferences, with participants expressing stronger concerns after the experiment than prior.

Overall, we expect the ongoing study to clarify a grey area surrounding user attitudes towards VR data collection. We hope these insights can inform future works on privacy in VR, clarify the need for PETs addressing risks of re-identification and inferences, and support the development of usable interfaces to inform users about data collection in VR.

Acknowledgments

This work received funding from PERSEUS, a EU Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement no. 101034240, and the Research Council of Norway through the SFI Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS) project no. 310105. We would like to thank all colleagues and participants who helped us with this pilot study.

References

[1] M. Abhiram and Amey Khare. Oculus Shooter Unity: A VR shooting simulator using Unity. https://github.com/NextTechLabAP/Oculus-Shooter-Unity, 2024. Accessed: April 2026.

[2] Sumit Asthana, Jane Im, Zhe Chen, and Nikola Banovic. "I know even if you don't tell me": Understanding Users' Privacy Preferences Regarding AI-based Inferences of Sensitive Information for Personalization. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI '24, New York, NY, USA, 2024. Association for Computing Machinery.

[3] European Commission, Content Directorate-General for Communications Networks, Technology, Visionary Analytics, C. Boel, K. Dekeyser, F. Depaepe, L. Quintero, T. v. Daele, and B. Wiederhold. *Extended Reality – Opportunities, Success Stories and Challenges (Health, Education) – Final Report*. Publications Office of the European Union, 2023.

[4] Florian M. Farke, David G. Balash, Maximilian Golla, and Adam J. Aviv. How Does Connecting Online Activities to Advertising Inferences Impact Privacy Perceptions? *Proceedings on Privacy Enhancing Technologies*, 2024(2):372–390, April 2024.

[5] Gonzalo Munilla Garrido, Vivek Nair, and Dawn Xiaodong Song. SoK: Data Privacy in Virtual Reality. *Proceedings on Privacy Enhancing Technologies*, 2023.

[6] Hilda Hadan, Derrick M. Wang, Lennart E. Nacke, and Leah Zhang-Kennedy. Privacy in Immersive Extended Reality: Exploring User Perceptions, Concerns, and Coping Strategies. *Conference on Human Factors in Computing Systems - Proceedings*, 2024.

[7] IEEE SA Industry Connections. The IEEE Global Initiative on ethics of Extended Reality (XR) Report - Extended Reality (XR) and the erosion of anonymity and privacy. Technical report, IEEE, 2021.

[8] Emiram Kablo, Melina Kleber, and Patricia Arias Cabarcos. *PrivaCI in VR: exploring perceptions and acceptability of data sharing in virtual reality through contextual integrity*, chapter 80, page 1531–1548. USENIX Association, USA, 2025.

[9] Mark Roman Miller, Fernanda Herrera, Hanseul Jun, James A. Landay, and Jeremy N. Bailenson. Personal identifiability of user tracking data during observation of 360-degree vr video. *Scientific Reports*, 10(1), October 2020.

[10] Vivek Nair, Wenbo Guo, Justus Mattern, Rui Wang, James F. O'Brien, Louis Rosenberg, and Dawn Song. Unique identification of 50,000+ virtual reality users from head & hand motion data. In *Proceedings of the 32nd USENIX Conference on Security Symposium*, SEC '23, USA, 2023. USENIX Association.

[11] 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(4):238–256, October 2023.

[12] Vivek Nair, Christian Rack, Wenbo Guo, Rui Wang, Shuixian Li, Brandon Huang, Atticus Cull, James F. O'Brien, Marc Latoschik, Louis Rosenberg, and Dawn Song. Inferring Private Personal Attributes of Virtual Reality Users from Ecologically Valid Head and Hand Motion Data . In *2024 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pages 477–484, Los Alamitos, CA, USA, March 2024. IEEE Computer Society.

[13] Pier Paolo Tricomi, Federica Nenna, Luca Pajola, Mauro Conti, and Luciano Gamberini. You can't hide behind your headset: User profiling in augmented and virtual reality. *IEEE Access*, 11:9859–9875, 2023.

[14] Lynne Warin, Viktoriya Pak, and Delphine Reinhardt. Privacy Perceptions Across the XR Spectrum: An Extended Reality Cross-Platform Comparative Analysis of A Virtual House Tour. *Proceedings on Privacy Enhancing Technologies*, 2025(1):150–168, January 2025.