Immersive Privacy and Security Awareness

JiHo Lee*
Virginia Tech
Blacksburg, Virginia, USA
jiholee@vt.edu

Carissa Bostian*
Virginia Tech
Blacksburg, Virginia, USA
carissab@vt.edu

Mughees Ur Rehman*
Virginia Tech
Blacksburg, Virginia, USA
mughees@vt.edu

Abstract

As virtual environments (VEs) become more integrated into daily life, users are increasingly exposed to invisible data collection mechanisms, often without full understanding or meaningful consent. This study investigates how immersive and interactive VR experiences can be leveraged to improve user awareness of privacy policies and data collection practices. We designed two types of VR privacy rooms: a mirror-based room with low interactivity and a game-based room with high interactivity—each focusing on eye tracking, emotion tracking, and hand tracking. Through a within subjects study, participants experienced both approaches and were assessed through comprehension quizzes, Likert-scale evaluations, and open-ended feedback. Our results show that the game-based rooms significantly outperformed mirror-based ones in enhancing user understanding, perceived transparency, and caution toward data sharing. Participants in the interactive condition achieved higher quiz scores, reported greater awareness of data tracking, and expressed increased skepticism about third party data use. These findings suggest that integrating privacy education into interactive VR systems can be an effective approach to informing users and empowering informed decision-making in immersive contexts. The APK files for the mirror-based and game-based approaches can be found https://github.com/Mughees2001/Immersive-Privacy-and-Security-Awareness.

CCS Concepts

• **Security and privacy → Usability in security and privacy**; • **Human-centered computing** → *Virtual reality*; *User studies*; Interaction design process and methods.

Keywords

Privacy, Security, Awareness, Immersive, Technology, User Experience, Security Awareness, Digital Privacy, Interactive Learning

ACM Reference Format:
JiHo Lee, Carissa Bostian, and Mughees Ur Rehman. 2018. Immersive Privacy and Security Awareness. In *Proceedings of Make sure to enter the correct conference title from your rights confirmation email (Conference acronym 'XX).* ACM, New York, NY, USA, 8 pages. https://doi.org/XXXXXXX.XXXXXXX

*The authors contributed equally to this research.

Conference acronym 'XX, Blacksburg, VA

ACM ISBN 978-1-4503-XXXX-X/2018/06
https://doi.org/XXXXXXX.XXXXXXX

1 Introduction

As virtual environments (VEs) are becoming increasingly sophisticated and have begun to be integrated into everyday life, concerns regarding data security and user privacy have arisen. Many users often lack awareness of the extent to which their data is being collected. Although user consent and acknowledgment forms aim to educate users on this information, users frequently skim or bypass them entirely due to their length, complexity, and use of legal jargon. Consequently, the majority of users are unaware of what data is being collected, and more importantly, how this data may be used to target them. This research aims to bridge the gap between user perceptions and the reality of data collection and use in VEs. Through educating users on the implications of skimming or skipping the lengthy, confusing consent forms, this study seeks to enhance user awareness of the risks associated with data collection. Further, this project seeks to explore how the conventional consent methods fail to effectively deliver key information to VE users and explores strategies for enhancing user awareness. Finally, this research seeks to promote transparency and empowers users to make informed decisions so they can better protect themselves and their data.

2 Background and Motivation

Privacy risks in VEs have become increasingly complex as these technologies have grown more immersive and ask for more data permissions. Current privacy policy consent mechanisms are often lengthy and text-heavy, resulting in them failing to engage users or properly convey meaningful information. Prior research highlights that users rarely read or fully comprehend these documents, leaving them unaware of what personal data is being collected or how it may be used. This lack of awareness is especially problematic in VEs, where systems routinely capture sensitive behavioral and biometric data. Additionally, VE users are unaware to the extent to which this data is unique to them and how it can be used to identify them. Motivated by the need for more effective and user-friendly privacy education, this research explores interactive, game-based alternatives to traditional consent forms to promote awareness, transparency, and user agency in data-driven virtual spaces.

3 Related Works

Oftentimes, users are unaware of the extent to which their data is being collected, stored, and used. Further, they do not understand the consequences they may face if their data ends up in the wrong hands. Meanwhile, the exponentially growing interest in Virtual Environments (VEs), which often use Head Worn Devices (HWDs) equipped with various sensors, poses risks of user data exposure. With this growing concern, researchers have explored the various data collection methods used in VEs to better understand associated

privacy risks. There has also been research on users' perceptions of these risks, finding that users are often unaware of the breadth of information collected or its misuse potential.

Recent studies underscore the need for targeted education and improved user interfaces specifically designed for privacy comprehension in VEs. There have been study that reported significant gaps in user understanding regarding involuntary biometric data collection, such as heart rate, and involuntary gaze patterns, highlighting the need for clearer communication about the potential sensitivity of this data [4] . Similarly, another study found that traditional 2D privacy policies fall short in VE due to their complexity and lack of interactivity [8]. They recommend leveraging immersive affordances unique to VR. Specifically, they suggest interactive consent mechanisms that engage users directly within the VE itself to enhance comprehension and informed decision making.

Advancements in technology have allowed VR systems to create real-time 3D avatars of a user in a VE. Powered by user biometric data, such as eye gaze and facial expressions, these systems can accurately mimic a user's real-world expressions [11] for the user's immersive experience. With the addition of body position tracking, full user avatars can be generated in real-time. Most users are blinded by the excitement of this technology and often overlook the various risks that data collection poses. These risks include unauthorized data collection, lack of transparency regarding data usage, and misuse of sensitive user data [3, 1]. A major user privacy concern involves the collection of eye gaze and body movement data, as it can be exploited for unauthorized user identification [1]. While Privacy-Enhancing Technologies (PETs) exist, they are incompatible with VE systems due the requirement for always-on sensing to be enabled for user immersement [1, 6]. A common gap among current research is the lack of a standardized privacy regulation for VE systems.

For user awareness of data collection and usage, attempting to read and understand privacy policy is crucial for mitigating risks. However, users are often prone to skip text- based privacy policies due to complex jargon and lengthy content [5]. Even when read, these website privacy policies demand spending significant time on understanding the content making big tradeoffs between time and economic cost [5]. Text-based privacy policies in the VR domain are especially complex, as they involve relatively large data collection and processing, making the contents extremely complicated [10]. Thus, understanding these privacy policies and informed user consent in VR is crucial yet underexplored.

There have been different methods beyond text-based privacy policies, such as video-based interfaces, which could be implemented to engage users in understanding more effectively [2]. Other approaches include showing privacy indicators within applications. Displaying short, relevant privacy notices helps users understand how their data is collected and used [7]. Similar to the video-based interface approach, an alternative method is to use interactive games. One group of researchers proposed a game-based approach to privacy awareness in VR, showing that immersive, interactive experiences can improve users' awareness and control over data collection[9]. Inspired by their findings, our project adopts some of this strategy by using a VR game format to engage users in understanding privacy risks. Users are unaware of the risks they face by providing these systems access to extra sensory data. In this project, we aim to educate users interactively within VE systems to aid them better understand data practices and reduce privacy risks.

4 Research Goal and Research Questions

Our research goal is to develop an interactive VR room that effectively informs users about privacy policies and raises awareness of data collection practices within VEs. By integrating privacy concepts into immersive game play, the study aims to explore whether a game-based approach can improve user understanding, engagement, and trust compared to more traditional, passive methods.

To effectively measure the quality of our findings, we pose the following research questions:

- **RQ1**: How users gain awareness of data collection from the game-based VR room compared to mirror-based version?
- **RQ2**: Is the game-based VR room more effective and engaging in delivering privacy concepts?
- **RQ3**:Does game approach influence how users trust, understand, or value the privacy policy?

5 Methodology

To address the research questions on how immersive and interactive environments influence user understanding of privacy policies in Virtual Environments (VEs), we designed and implemented two distinct types of VR experiences: a mirror-based room (low interactivity) and a game-based room (high interactivity). Each approach was further divided into three specialized rooms focusing on different types of user-tracked data: eye tracking, emotion tracking, and hand tracking. We conducted a pre-survey and a post-survey to observe changes in user behavior before and after experiencing the mirror-based VR room and the game-based room. Our study framework has been demonstrated in Figure 1.

5.1 Privacy Room Design Decision

Mirror-based approach The mirror-based rooms offer a less interactive, observational experience where the user is presented with feedback about their data being collected, but with minimal required input.

- Eye Tracking Room: A visual ray is emitted from the user's eye gaze direction, allowing them to see precisely what the system is tracking as they move their gaze. The room simulates passive observation of gaze tracking. This is demonstrated in Figure 2 (a) & (b).
- Emotion Tracking Room: An avatar is placed in front of the user, mimicking their real-time facial expressions. This aims to make users aware of how emotional data can be captured and represented. This is demonstrated in Figure 3 (a) and (b).
- Hand Tracking Room: Virtual hands inside the room mirror the user's real hand movements, demonstrating the fidelity and responsiveness of hand-tracking systems. Additionally, the users' virtual hands are reflected in a mirror on the wall to further increase their awareness of how their hand movement is used. This is demonstrated in Figure 4 (a).

Game-based approach The game-based rooms introduce interactive elements and tasks to engage users in exploring how their data

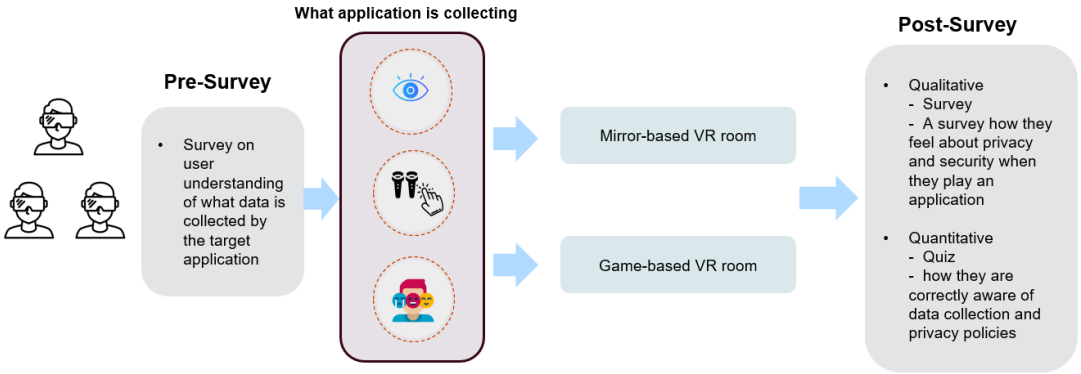


Figure 1: Framework – Immersive Privacy and Security Awareness

is being collected and used. Each room provides real time feedback based on the user's actions.

- Eye Tracking Room: Users are presented with six artworks. As they look at each image, the system records the gaze duration. After a fixed period, they are shown which painting they viewed and the corresponding viewing time in seconds. It captures subtle user interactions, revealing preferences and providing insights into visual attention and decision-making. This is demonstrated in Figure 2 (c) and (d). This game-based room was developed after several revisions. The previous versions of this room are shown in the appendix section.
- Emotion Tracking Room: A short video is played in the environment. While the user watches, their facial expressions are tracked. Upon video completion, the system summarizes the user's dominant emotional response, highlighting the sensitivity of expression analysis. This is demonstrated in Figure 3 (c).
- Hand Tracking Room: The user is prompted to sign their name in the air using hand gestures. After the signature is completed, the room displays a notification informing the user that this biometric signature can be stored and used, emphasizing consent and potential misuse. This is demonstrated in Figure 4 (b) and (c).

These six rooms were carefully designed to expose participants to both passive and interactive experiences of privacy-sensitive data collection, enabling comparison of comprehension and engagement between the two approaches.

5.2 Implementation

The rooms were developed using Unity (version 2022.3.52f1) with the OpenXR package to ensure cross-platform VR compatibility. All experiences were run on Meta Quest Pro headsets, leveraging its advanced capabilities in eye tracking, facial expression detection, and hand tracking. Development and version control were managed using Unity Cloud and Unity Version Control. Each room was instrumented to log user behaviors, system responses, and timestamps to enable quantitative evaluation.

5.3 Study Design

We conducted a within-subjects study where participants experienced both the mirror-based and game-based rooms. Room order was counterbalanced to reduce learning effects. After each room, participants completed a short quiz to assess comprehension of privacy concepts and a survey on perceived awareness and engagement.

The user study included five participants all withing the age range of 22 to 37 years old with an average age of 29.0 years (SD = 5.3). This modestly diverse age range allowed us to gather perspectives from both younger and slightly older adult users. In terms of VR technology familiarity, 3 participants expressed a high level of comfort with the technology.

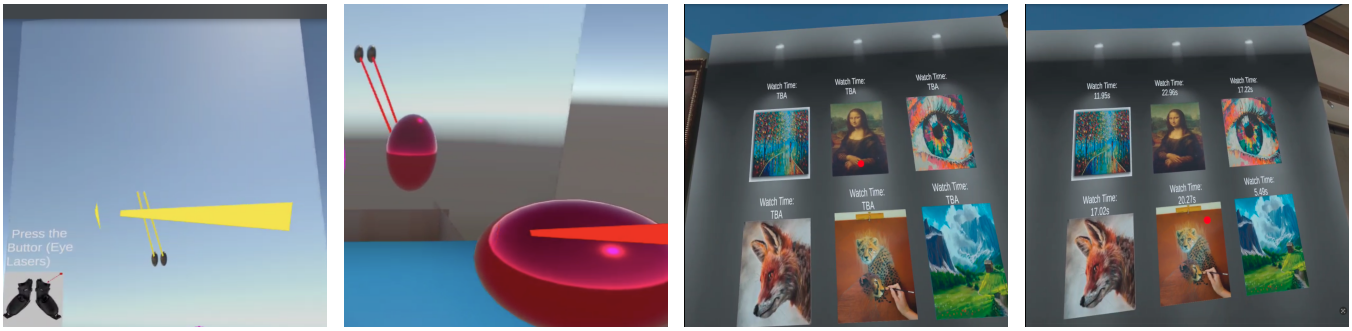
6 Evaluation

The primary findings of our study indicated that there is an overall improvement in understanding and satisfaction among participants when using the game-based approach. To provide detailed results and findings, we categorized them into three key sections: quantitative results, qualitative results, and feedback from participants.

6.1 Quantitative Results

The result is based on the responses from the quiz section of the questionnaire, which consisted of n multiple choice questions. These questions were designed to assess the participants' understanding of the app's privacy policies, covering topics such as the kind of data being collected, and purpose/reasons for such information being collected, whether it was mandatory to give such data.

6.1.1 Overall Result. The total score of the quiz sections on the questionnaire in Fig. 5 indicated a higher understanding of privacy policies with the use of the game-based privacy policy room. The average score for participants using the mirror-based privacy policy rooms was 3.6 out out 7, whereas this average was higher in the interaction-based privacy policy rooms with 6.2 out of 7. The standard deviation for both designs were 1.34 and 1.10, respectively. These findings align with our initial hypothesis that the game-based privacy policy room being more interactive and engaging would result in better user comprehension than the mirror-based room.

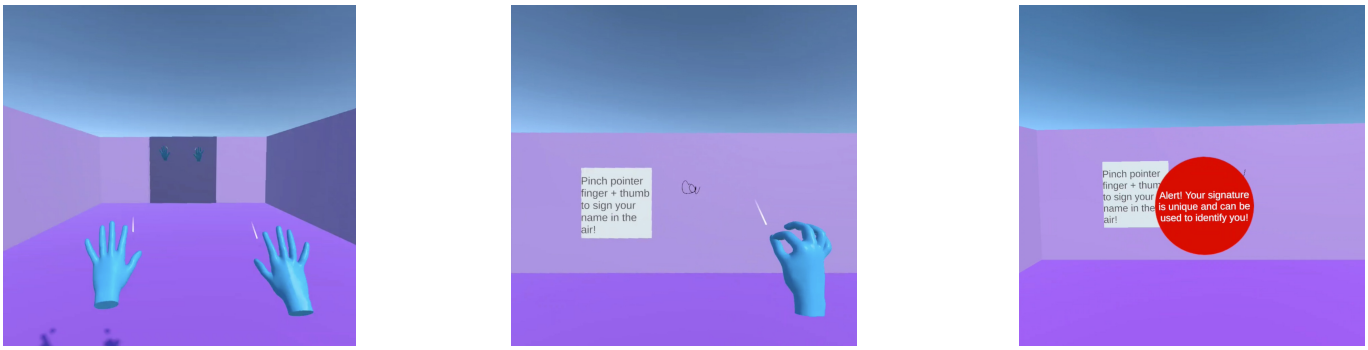


(a) (b) (c) (d)

Figure 2: (a) and (b) illustrate the Eye Gaze Mirror-Based Approach. (a) depicts two eyeballs with rays that move in sync with the eyeballs. (b) shows the eyes interacting with an object, where the color of the ray changes upon interaction. (c) demonstrates the Eye Tracking Game-Based Approach, where initially all paintings display TBA (To Be Announced) time, awaiting user interaction. (d) indicates the watch time for each painting, representing the total duration spent observing it.

(a) (b) (c)

Figure 3: (a) Representation for emotion tracking in mirror-based approach with smiling facial expression of an user (b) Representation for emotion tracking in mirror-based approach with opening mouth facial expression of an user (c) Representation for emotion tracking in game-based approach with dominant facial expression of an user after watching short video



(a) (b) (c)

Figure 4: (a) Represents the hand tracking mirror approach. (b) Represents the hand tracking game approach, where users are instructed to sign their name in the air. (c) Shows an alert that pops-up after the user signs their name, informing them that their signature is a unique identifier.

6.1.2 Results for Each Features. Fig 6 shows that participants demonstrated consistently higher understanding of privacy purposes for each features. Eye tracking showed the most difference between mirror-based and interaction-based room. Participants in the interaction-based room scored 2.0, compared to just 0.6 in the

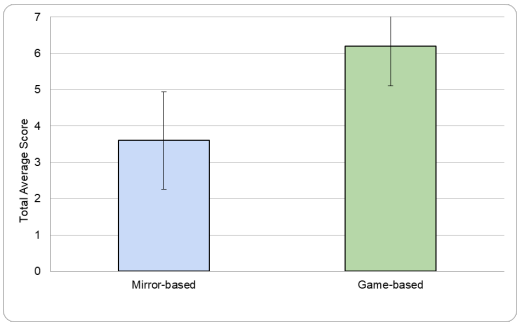


Figure 5: Average total score of questionnaires regarding privacy purpose for mirror-based and interaction-based approach respectively

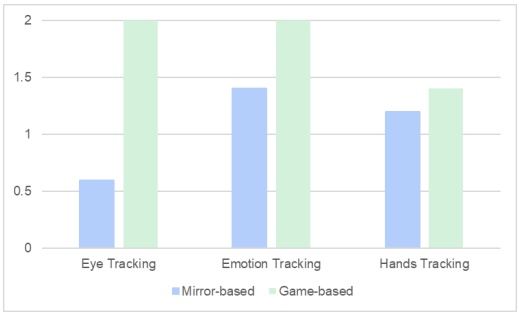


Figure 6: Average score of questionnaires regarding privacy purpose for each features

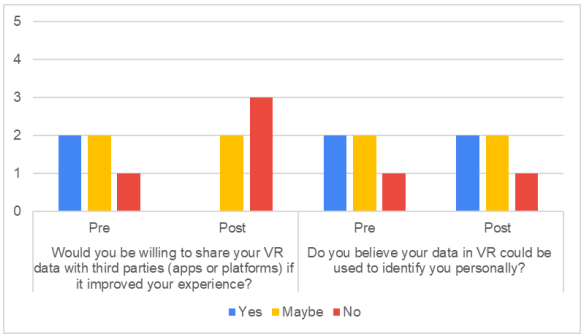


Figure 7: The number of responses for trust level for VR applications before and after our privacy informing rooms

Figure 8: Average Likert score of perceived awareness of data collection

mirror-based room. This suggests that the gave-driven image with art gallery images showing interest collects task was more effective in making users aware of how gaze data could reflect personal interest or attention patterns. For emotion tracking, score were also higher in the interaction-based room (2.0) compared to the mirror-based room with 1.4 average score. The immersive emotion response method summarizing dominant emotion helped participants better grasp the scope and sensitivity of facial expression tracking. In hand tracking, the difference was smaller with 1.2 and 1.4 respectively. This may because both mirror-based and interaction-based rooms provide a relatively clear visual representation of hand tracking, though the interaction-based approach introduced added context via the signature task and follow-up notification.

These results answer our RQ2 showing that interactive experiences enhance user awareness of data collection practices. Notably, the biggest learning gap appeared in the eye tracking room, which may indicate that the abstract or passive data like eye gaze behavior requires more strong visualization and contextualization to be understood.

6.2 Qualitative Results

We investigated how participants felt regarding privacy policy during using the mirror-based and game-based rooms followed by quantitative questionnaires to understand the satisfactory level of users. To measure shifts in user trust and awareness regarding VR data privacy policy, participants answers pre and post survey before and after experiencing the privacy awareness VR rooms.

Fig. 7 shows the responses for trust level for VR applications before and after our privacy informing rooms. For the question of willingness to share data with third parties, participants show that evenly distributed among "Yes," "Maybe," and "No" for an improved experience. However, after the experience, the number of "No" responses increased from 1 to 3, showing lowered trust. Also, the number of "Yes" responses dropped to 0, suggesting a significant loss of blind trust after the experience. The more participants aware and understand the privacy policy, the more participants reluctant to share their data. This imply that users understand potential risk with further analysis beyond their simple collection.

For the question of whether users believe their VR data could be personally identifying them, the distribution of responses remained unchanged before and after the experience. This suggests that while users' feelings toward sharing data changed, their belif about the identifiability of VR data was already formed and less influenced by the experience.

These finding answer our RQ1 broadly, supporting the notion that interactive privacy education in VEs can impact user decision-making and their awareness.

Fig. 8 shows higher average Likert scale in game-based approach for perceived awareness. The mirror-based room with an average of 3.2 indicates moderate level of awarness. The game-based room shows a higher average of 4.8, indicating that participants felt

highly aware of the data being collected during that experience with purpose understanding.

These answers our RQ2 amd RQ3 underscoring the effectiveness of interactive feedback privacy policy education. In the game-based rooms, features such as real-time feedback with user interest of viewed images, emotion summaries, consent messages appear to have made data collection purpose more transparent to users. Thus, the mirror-based experience, while informative, lacked the same level of engagement and contextual feedback.

6.3 Feedback

Lastly, we collected feedback on our study designs after participants finished experiencing both mirror-based and game-based approach included in post-survey questionnaires. Participants were asked open-ended questions regarding their perceptions of the VR privacy experience.

Was the experience worth the privacy trade-off with time consumed? 3 out of 5 participants explicitly responded "Yes". They felt that the experience was informative, educational, and engaging. However, 2 participants were unsure, expressing skepticism about whether the data being collected was significant enough to justify concern.

Did the experience change your opinion about sharing personal data in VR? 2 participants answered that their opinion had changed. They express that the extent of data such as user interest inferred from seemingly benign data is concerend.

General feedback on the study One participant described the experience as "*beyond what I thought*", especially with respect to biometric data such as signatures and inferred emotional states. Several participants said that the game-based approach was engaging and educational, one calling it an "*interesting idea to learn privacy policy by playing a game.*" Notably, one participants remarked, "*I fell VR apps are suspicious now*"

These qualitative responses suggest that the VR experience effectively prompted reflection, awareness, and even attitude change in some users. While not all participants were convinced to change behavior, most acknowledged a deeper understanding of how VR data can be used or misused.

7 Discussion

Our findings demonstrate that game-based VR environments are more effective in raising user awareness of data collection practices than passive, mirror-based experiences. Participants who interacted with the game-based rooms showed higher comprehension scores, greater perceived awareness, and more hesitation about opting into data sharing. These results suggest that interactive, immersive based awareness methods not only enhance ones understanding of complex privacy policy concepts, but they also influence how willing users are to opt into sharing their data. While both the mirror-based and game-based approaches revealed certain privacy insights, the game-based rooms offered contextualized feedback that made data collection more tangible and personal. This supports the idea that embedding privacy education into interactive tasks can bridge the gap between user perception and the realities of data collection in VEs.

8 Conclusion and Future Work

Our study showed that high interactive, game-based VR privacy policy education room improve users' understanding and awareness of privacy policies compared to passive, mirror-based environments. Participants in the game-based rooms scored higher average on comprehension quizzes, felt improved awareness of data collection practices, and expressed reluctance toward sharing their personal data with third parties. The notable difference were shown in the eye-tracking features, where visual feedback and personalized interaction effectively highlighted how subtle behavioral data could reveal user preferences. Qualitative feedback further demonstrated that participants found the interactive experiences more informative, memorable, and engaging. This suggests that immersive learning of privacy policies can foster more critical attitudes toward data privacy and user decision-making in VEs.

For future work, there are several promising directions to extend this research. Instead of isolating sensor types: eye tracking, emotion tracking, and hand tracking—future studies could integrate multiple sensors simultaneously within a single immersive environment. Additionally, exploring the other sensory inputs, such as voice recognition through microphone sensors, could significantly enrich user understanding of privacy risks. Adding features such as voice, head and surroundings withing a single experience would enable users to see the broader scope of data being collected and how it may be cross-analyzed. For example, future studies could implement scenarios where users experience their own voice recordings played back within the VR environment, highlighting potential misuse and the identifiable nature of vocal data. To make the user study more concrete, we can focus on examining the long term impacts of interactive privacy education. Conducting studies over an extended period would reveal whether the increased awareness gained from interactive experiences leads to lasting behavioral changes in privacy practices. Further, more efficient way of game-based VR privacy rooms can be designed with reduced learning time.

References

[1] Samantha Aziz and Oleg Komogortsev. 2025. Exploring the uncoordinated privacy protections of eye tracking and vr motion data for unauthorized user identification. In *2025 IEEE Conference Virtual Reality and 3D User Interfaces (VR)*. IEEE, 217–227.

[2] Pascal Faurie, Arghir-Nicolae Moldovan, and Irina Tal. 2020. Privacy policy–"i agree"?!–do alternatives to text-based policies increase the awareness of the users? In *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. IEEE, 1–6.

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

[4] Hilda Hadan, Derrick M. Wang, Lennart E. Nacke, and Leah Zhang-Kennedy. 2025. Privacy in immersive extended reality: exploring user perceptions, concerns, and coping strategies. *arXiv preprint arXiv:2503.21010*. https://arxiv.org/abs/2503.21010.

[5] Aleecia M McDonald and Lorrie Faith Cranor. 2008. The cost of reading privacy policies. *Isjlp*, 4, 543.

[6] 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, 1–35.

[7] Shidong Pan et al. 2024. A {new}{hope}: contextual privacy policies for mobile applications and an approach toward automated generation. In *33rd USENIX Security Symposium (USENIX Security 24)*, 5699–5716.

[8] Viktorija Paneva, Verena Winterhalter, Naga Sai Surya Vamsy Malladi, Marvin Strauss, Stefan Schneegass, and Florian Alt. 2025. Usable privacy in virtual

worlds: design implications for data collection awareness and control interfaces in virtual reality. *arXiv preprint arXiv:2503.10915*. https://www.arxiv.org/abs/2503.10915.

[9] Viktorija Paneva, Verena Winterhalter, Naga Sai Surya Vamsy Malladi, Marvin Strauss, Stefan Schneegass, and Florian Alt. 2025. Usable privacy in virtual worlds: design implications for data collection awareness and control interfaces in virtual reality. (2025). https://arxiv.org/abs/2503.10915 arXiv: 2503.10915 [cs.HC].

[10] Abhinaya SB, Abhishri Agrawal, Yaxing Yao, Yixin Zou, and Anupam Das. 2025. " what are they gonna do with my data?": privacy expectations, concerns, and behaviors in virtual reality. *Proceedings on Privacy Enhancing Technologies*, 2025, 1, 58–77.

[11] Guoxian Song, Jianfei Cai, Tat-Jen Cham, Jianmin Zheng, Juyong Zhang, and Henry Fuchs. 2018. Real-time 3d face-eye performance capture of a person wearing vr headset. In *Proceedings of the 26th ACM international conference on Multimedia*, 923–931.

A Prior Development of VR Game-Based Approach Rooms

This section covers the prior development of VR game-based approach rooms. All the updated and latest rooms are mentioned in Section 5.1.

A.1 Eye Tracking

Implementation Version 1. For the Eye Gaze Game-Based approach, we initially had a game where users had to use their eye gaze to type out a PIN (5 digits randomly generated). See Figure 9 for this, where:

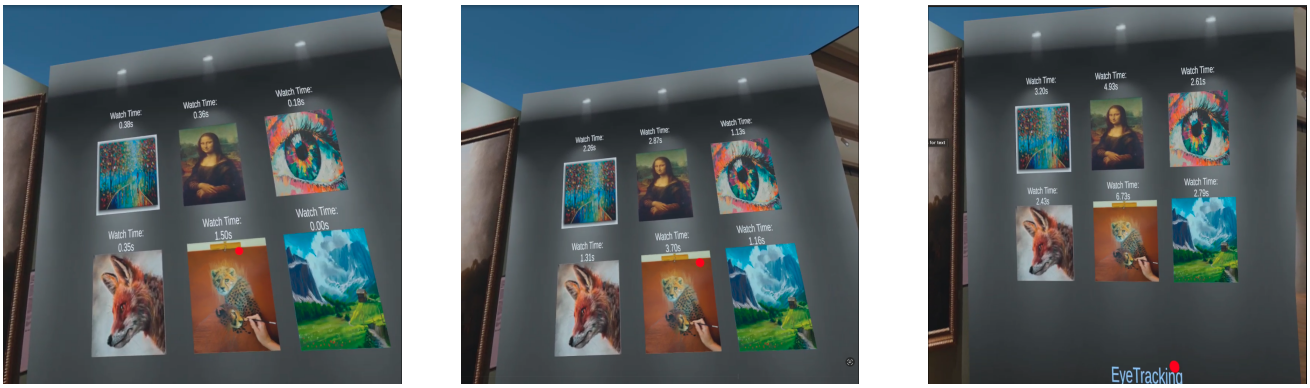
- (a) represents the goal *64795*,
- (b) represents the partially typed number *647* using eye gaze
- (c) Shows the successful completion.

Implementation Version 2. In the second phase, after receiving feedback, we implemented an art gallery scene. In this scene, the user is shown six different paintings famous across the world. Each painting has a live timer that records the time spent viewing it. The scene starts with all paintings showing a time of 0 seconds, which updates progressively as the user looks at each painting. The timer is updated live in front of the user. See Figure 10 for this.

Implementation Version 3. Modified the art gallery scene from version 2. As the user looks at each image, the system records the gaze duration. After a fixed period, they are shown which painting they viewed and the corresponding viewing time in seconds. It does not have a live timer that shows the timer updating on the fly, but at the end, it reveals which was your favorite painting (highest watch time), demonstrating the collection of eye gaze data. This has been demonstrated in Figure 2.

(a) (b) (c)

Figure 9: (a), (b), and (c) represent different stages of the Eye-Tracking Game-Based Approach. These images show the visual feedback of how the user's gaze interacts with the numpad in the game environment.



(a) (b) (c)

Figure 10: (a) represents the scene at the start when paintings have roughly 0 seconds of watch time. (b) shows the progression after the user has watched some paintings. (c) also depicts that the live time on paintings is being updated.