Interpreting Privacy Expectations in Virtual Environments

UC San Diego — JACOBS SCHOOL OF ENGINEERING

ERSP — UC San Diego Early Research Scholars Program

UJIMA — SECURITY & PRIVACY

Runpeng Jian, Jared Jose, Molly MacLaren, Zheng Zeng

Advisors: Mya Bolds, Jay Jhaveri, Imani N. S. Munyaka

Background

Virtual environments are digitally simulated experiences that have begun to leverage virtual reality (VR) equipment to make environmental interactions more immersive.
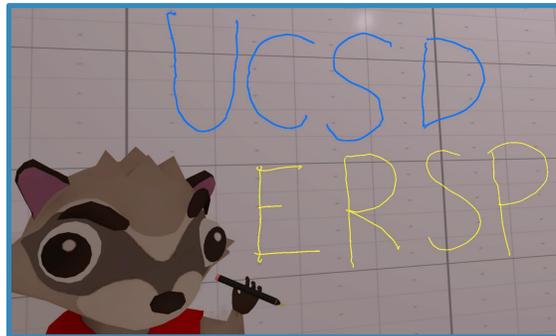
Figure 1. VRChat user interacting with a whiteboard.

The **metaverse** is a broad term for shared virtual environments which seek to prioritize seamless interconnectivity between users.
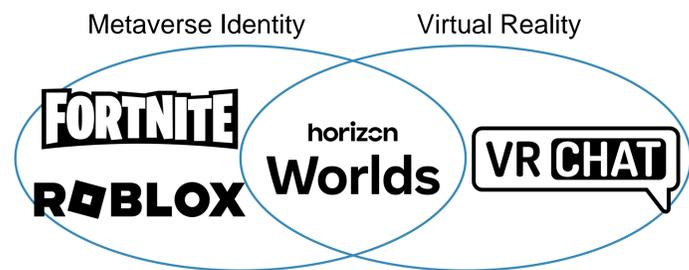
Figure 2. Virtual environment platforms studied.

Motivation

- The functionality of shared virtual environments is highly **dependent on user data**.
- End user expectations of security and privacy may be **different** from reality.
- Identifying where these discrepancies lie aids understanding how to **improve overall user experience**.
- Privacy expectations for **children** are different than expectations for other demographics.

Research Questions

- What are the **privacy expectations of users** in virtual environments?
- Are these expectations **reflected** in the **privacy policies** of these applications?

Methodology

Vignette Survey

- Examples of **real privacy situations** that users could potentially come across.
- Vignette structure allows the user to come to **their own conclusions on their beliefs** rather than have their beliefs given to them by a question.

Raw infrared face photos taken → Photos processed into datapoints → CPU → Datapoints sent to game server → Avatar facial expression displayed
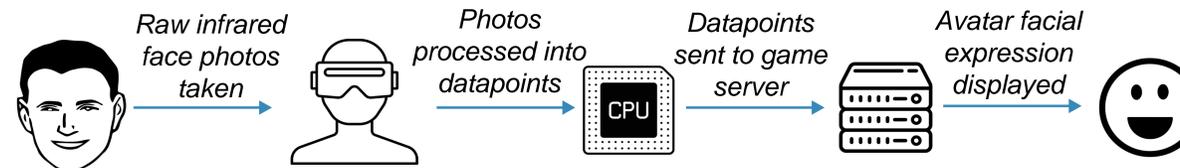
Figure 3. Diagram of a vignette: "Does this process meet your privacy expectations?"

Privacy Policy Analysis

- Qualitative evaluation highlights whether individuals can **extract important privacy information** from a given privacy policy.
- Quantitative evaluation utilizes the **Flesch-Kincaid** score to determine the general readability of privacy policies as it correlates to grade level.

Results

Survey Response Analysis
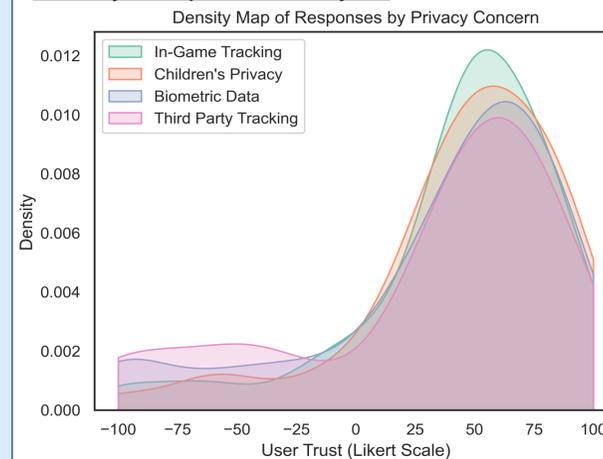
Figure 4. Distribution of responses by category.
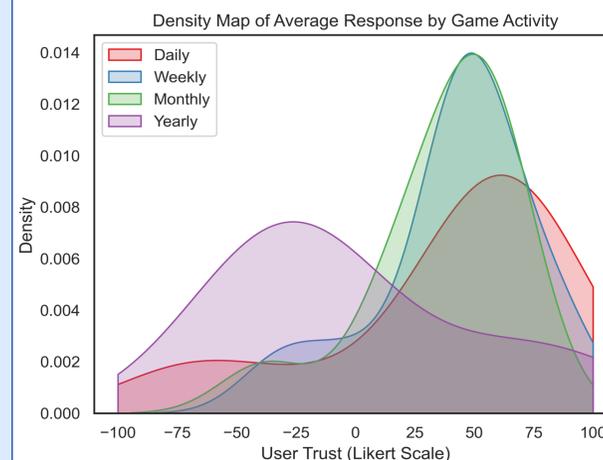
Figure 5. Distribution comparing privacy satisfaction among users with different frequencies of virtual environment interaction.

Privacy Policy Analysis

Category	Fortnite	Roblox	VRChat	Horizon Worlds
Allows for Data Control	✓	✓	✓	✓
Addresses Child Safety	✓	✓	✓	
Accessible	✓	✓	✓	
Language Availability	✓			
Ensures Third Party Protection		✓		
Notifies User of Data Breach		✓		
Collects Only Functional Data				

Figure 6. Examples of criteria analyzed.
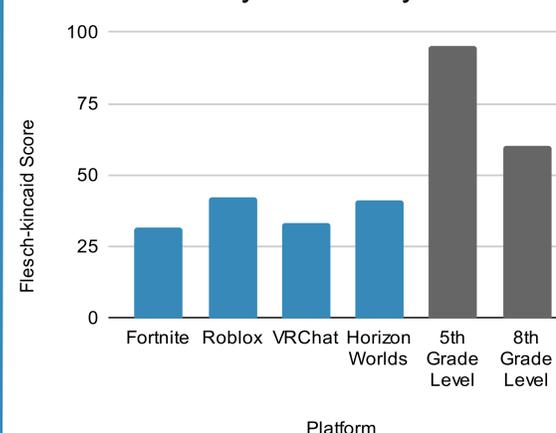
Figure 7. Policy reading comprehension with expected comprehension scores at grade level.

Conclusion

- Those who use virtual environments **more frequently** are more willing to **give up aspects of privacy** for **greater immersion**.
- Users are **most confident** in **in-game data tracking** and **children's privacy**, both categories which are well defined in most policies.
- Users are **less confident** in how these platforms handle **third party tracking** and **biometric data.**
- While most policies studied clearly define how data is used, they all collect **more data than what is required** for the platform to function.

Future Work

- Conduct **interviews** to gain a deeper understanding about user responses.
- Analyze social media posts using **NLP** to find which privacy aspects are discussed most among users and parents of underage users.
- Investigate "**dark patterns**" (intentionally misleading UX design) within VR environments.

Figure 8. Word cloud of survey responses to "Who is responsible for protecting privacy in gameplay?" Participant answers are split between the player and the company.

Acknowledgement