NC STATE UNIVERSITY

"What are they gonna do with my data?"

Privacy Expectations, Concerns, and Behaviors in Virtual Reality

Abhinaya S.B., Abhishri Agrawal, Yaxing Yao, Yixin Zou, Anupam Das

North Carolina State University

UNC Chapel Hill

Johns Hopkins University

Max Planck Institute for Security and Privacy

Presented at the 25th Privacy Enhancing Technologies Symposium (PETS), 2025

Socializing

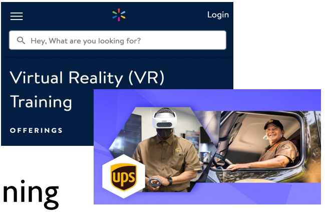
Productivity

Streaming

3D design & modeling

Gaming

360-degree immersive experiences



Virtual training

Privacy Risks Aplenty!

- User identification from motion, biometric data, and usage patterns with high accuracy
- Sensitive inferences about user attributes such as physical/mental conditions, emotions and personality
- Usage patterns used to influence purchase decisions
- Extraction of sensitive data such as passwords through keystroke inference attacks and remote keylogging attacks

VR User Privacy: Then Vs Now

VR User Concerns in 2018 (Adams et al., SOUPS 2018):

- Well-being (physical, psychological, etc.)
- Privacy:
  - Data collection from camera/microphone sensors
  - Reputation of headset manufacturer

VR landscape now:

- Growth in market, user base, affordable headsets
- New VR use cases such as virtual desktops, erotic role-play

[1] Devon Adams, Alseny Bah, Catherine Barwulor, Nureli Musaby, Kadeem Pitkin, and Elissa M Redmiles. 2018. Ethics emerging: the story of privacy and security perceptions in virtual reality. In Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018). 427–442

VR User Privacy: A Re-evaluation

Semi-structured interviews

Active users of VR applications

- **RQ1:** What are VR users' expectations of privacy and data practices in VR?
- **RQ2:** What are VR users' privacy concerns and reasons for not having concerns?
- **RQ3:** What are VR users' practices to manage their privacy in VR and reasons for not having privacy-protective practices?

Study Design

125 valid responses to screening survey; 20 completed interviews

Recruitment

- VR-specific subreddits
- Facebook groups
- Discord servers
- Snowball sampling

Requirements

- At least 18 years old
- Residing in the US
- Current user of at least one VR application

Screening survey questions

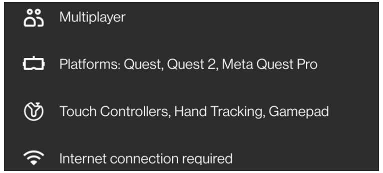
- VR usage: frequency, duration, headsets used, activities performed
- Demographics

Participants verified to be VR users by checking their headsets through webcam before interview

Study Design: Interviews

- Presented screenshots containing data collection information in VR apps used by participants
- Showed logos & branding of popular VR products to elicit participant perception about them

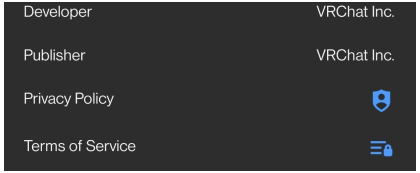
oculus
PlayStation.VR
VIVE
Pimax
SAMSUNG Gear VR
STEAM
VALVE INDEX
Daydream
HP REVERB G2
Meta Quest
Microsoft HoloLens


Multiplayer

Platforms: Quest, Quest 2, Meta Quest Pro

Touch Controllers, Hand Tracking, Gamepad

Internet connection required



Developer	VRChat Inc.
Publisher	VRChat Inc.
Privacy Policy	
Terms of Service	

RQ1:VR Users' Privacy Expectations

A Few Expectations of Data Collection and Usage

- Monetization of biometric data
- Demographic information collection for targeted VR app development
- User interests collected for targeted advertising within or outside VR
- Speculations about developers having access to the feed of users' personal living space

Understanding of Data Practices (Screenshot activity)

- Reactions varied; some data collection was expected and rationalized based on functionality
- Participants were confused/surprised when they couldn't identify a reasonable use case for certain data collection

RQ2:VR Users’ Privacy Concerns

Institutional Privacy Concerns

- Platform & App Surveillance
- Sale and sharing of data
- Perceived lack of regulations
- Trust and concern levels depending on company size, reputation and past privacy-violating practices

Social Privacy Concerns

- Eavesdropping and unauthorized recording by other users
- Impersonation: particularly of children/hard-of-hearing individuals
- Doxxing
- Cross-platform inferences based on linked social media

Device-related Privacy Concerns

- Leakage of confidential work data while using virtual desktop
- Leakage of sensitive data (e.g., passwords) while livestreaming
- Access to sensory data

RQ2: Reasons for Lacking Privacy Concerns

Institutional Privacy Concerns

Social Privacy Concerns

Device-related Privacy Concerns

- **Awareness** of data practices
- **Willingness** to share data for improving VR
- **Trust** in various entities of the VR ecosystem
- **Lack of perceived harm**

> “*Even if they knew all of my usage data on [device], what are they gonna do with it?*”

RQ3:VR Users' Privacy-protective Behaviors

Device-oriented Measures

- Purchase "privacy-friendly" VR headsets
- Minimizing device access to sensitive data

App-oriented Measures

- Checking data practices before app use
- Minimizing cross-platform inferences

Interaction-oriented Measures

- Avoiding disclosure of PII
- Limiting certain types of interactions

RQ3: Reasons for Lacking Privacy-protective Behaviors

Device-oriented Measures

App-oriented Measures

Interaction-oriented Measures

- **Lack of concern** and **limited awareness** of privacy implications
- **Economic considerations** in switching VR headsets
- Desire to continue **enjoying VR**

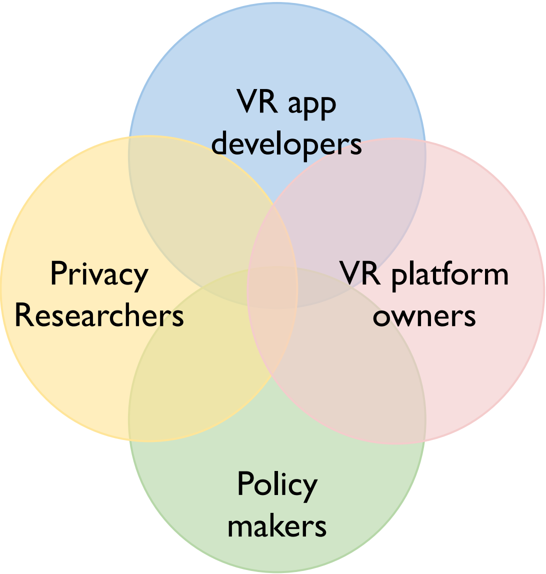
> “*It’s mildly embarrassing, but I usually continue to use the app… what am I going to do, make my own?*”

VR User Privacy: Misconceptions

- Underestimation of the types of sensitive data collected and their privacy implications
- Lack of awareness about advanced attacks (e.g., keystroke inference, remote keylogging)
- Misplaced concerns about "lack of regulations" for non-US VR products

Recommendations

Develop and integrate privacy controls and privacy-preserving techniques into VR systems



Privacy-focused onboarding tutorials; social media outreach

Diversification of the VR market

3rd party auditing on VR apps' and VR platforms' compliance with regulations

Thank You

Key Takeaways:

- VR users' privacy expectations reveal *misconceptions*
- VR users have several *institutional*, *social* and *device-related* privacy concerns
- They protect their privacy using *device-oriented*, *app-oriented* and *interaction-oriented* measures

Call to Action for stakeholders in the VR ecosystem:

- Reduce users' misconceptions about VR privacy through social media outreach and privacy-focused tutorials
- Conduct third-party auditing on VR apps' and platforms' compliance with regulations
- Develop privacy controls into VR systems
- Diversify the VR market to provide consumers with more choice for their privacy

Read our paper

Access our study materials

Contact:
asrivid@ncsu.edu
anupam.das@ncsu.edu