"*What are they gonna do with my data?*": Privacy Expectations, Concerns, and Behaviors in Virtual Reality

Abhinaya S.B.
North Carolina State University
asrivid@ncsu.edu

Abhishri Agrawal
UNC Chapel Hill
abhishri@unc.edu

Yaxing Yao
Virginia Tech
yaxing@vt.edu

Yixin Zou
Max Planck Institute for Security and Privacy
yixin.zou@mpi-sp.org

Anupam Das
North Carolina State University
anupam.das@ncsu.edu

Abstract

The immersive nature of Virtual Reality (VR) and its reliance on sensory devices like head-mounted displays introduce privacy risks to users. While earlier research has explored users' privacy concerns within VR environments, less is known about users' comprehension of VR data practices and protective behaviors; the expanding VR market and technological progress also necessitate a fresh evaluation. We conducted semi-structured interviews with 20 VR users, showing their diverse perceptions regarding the types of data collected and their intended purposes. We observed privacy concerns in three dimensions: institutional, social, and device-specific. Our participants sought to protect their privacy through considerations when selecting the device, scrutinizing VR apps, and selective engagement in different VR interactions. We contrast our findings with observations from other technologies and ecosystems, shedding light on how VR has altered the privacy landscape for end-users. We further offer recommendations to alleviate users' privacy concerns, rectify misunderstandings, and encourage the adoption of privacy-conscious behaviors.

Keywords

Privacy, virtual reality, qualitative analysis

1 Introduction

Virtual Reality (VR) technologies use head-mounted displays (HMDs), controllers, and full-body tracking to enable 360-degree virtual experiences for users. The new interaction modalities of VR provide users with new, immersive experiences when playing games, streaming videos, and socializing. Social VR apps allow users to engage in activities that are not possible in traditional 2D social media, such as virtual drinking and erotic role-play (ERP). VR also augments the use of laptops/PCs through virtual desktop apps.

While VR leads to new and improved experiences, it also creates unique security and privacy (S&P) challenges, due to the fine-grained and multi-modal tracking through sensors in the VR equipment (such as in HMDs) as well as the three-dimensional interactions in VR environments. Past research has revealed unauthorized monitoring of avatars, in-game access control, and scripting vulnerabilities [6, 94]. Identity theft in VR is a growing concern, with hyper-personalized avatars impersonating loved ones to elicit personal information [52]. Researchers were able to identify 95% of a group of VR users using simple machine learning models trained on less than five minutes of tracking data per person [65]. Head and body movements achieve highly accurate user-identification [38, 49, 67, 71]. As VR platforms collect information about avatars, mannerisms, and virtual assets, the potential to make sensitive inferences about users based on such data — ranging from interests, to physical/mental conditions [5, 70] — increases. Recordings of movement data can identify sensitive attributes (ethnicity, disabilities, political orientation) with more than 50% accuracy [68].

Several prior studies have elicited VR users' perceptions of privacy, highlighting concerns around "always-on" sensors [5] and self-disclosure in social VR [57]. Nonetheless, the VR landscape has evolved drastically since these earlier works — including a substantial growth of its market and user base [8], the emergence of affordable stand-alone VR headsets [25], and the advancement of VR for new use cases such as virtual desktops and erotic role-play. All of these factors call for a re-examination of users' privacy concerns. Moreover, there is limited knowledge of VR users' expectations of the data practices employed by VR devices/platforms, what actions they take to mitigate their privacy concerns, and the dynamics between such expectations, concerns, and behaviors.

We qualitatively examine three privacy-related constructs [18] for VR users: privacy *expectation* (what one views as the likely specific privacy-related outcome of a situation or behavior from the other parties involved), privacy *concern* (an expression of worry towards a specific privacy-related situation), and privacy *behavior* (what an individual actually does or has done in an attempt to achieve the level of privacy that they prefer).

Through semi-structured interviews with 20 active VR users, our study answers the following research questions:

RQ 1: *What are VR users' expectations of privacy and data practices in VR?* Participants believe a wide range of data, including physiological data and in-app interactions, to be collected. While these expectations largely align with the technical realities [63], the

Proceedings on Privacy Enhancing Technologies 2025(1), 58–77

https://doi.org/10.56553/popets-2025-0005

vague terms in privacy policies and other privacy-related information leave participants speculating on the exact types and purposes of data collection.

RQ 2: *What are VR users' privacy concerns and reasons for not having concerns?* Participants express three types of concerns: institutional (aimed at VR companies and regulators), social (related to other VR users), and device-specific (stemming from specific device features and use cases in VR). While reasons for the lack of privacy concerns overlap with non-VR contexts, such as the "I've got nothing to hide" sentiment [83], other reasonings are unique to VR, like the belief that VR devices are technically infeasible to be "always on."

RQ 3: *What are VR users' practices to manage their privacy in VR and reasons for not having privacy-protective practices?* Participants employ diverse privacy-protective strategies, such as careful device selection, verifying the app before usage, avoiding social account linking, and selectively engaging in different VR interactions.

Compared to prior academic literature on users' privacy concerns and behaviors around AR/VR, IoT, smartphones, and social media, our findings highlight **14** unique privacy concerns and **eight** unique privacy-protective practices (see Tables 1 and 2). Of these, we identify **seven** unique social privacy concerns (e.g., livestreaming of VR sessions by bystanders, impersonation of hard-of-hearing individuals, and digital stalking after VR interactions). In terms of privacy-protective practices, while some practices align with non-VR contexts, others are unique to VR, such as relying on heuristics for interacting in various VR spaces. Particularly, we highlight **13** previously unreported privacy-protective strategies in the VR environment (e.g., watching videos of VR app usage prior to installing the app, and obtaining permission from the security team before using VR for professional work).

We identify critical gaps in users' expectations of VR data practices that make them underestimate the privacy risks in VR. Specifically, most users do not consider the privacy implications due to the leakage of non-verbal (e.g., hand/motion) data about themselves. This calls for actions by VR platforms, app developers, and regulatory bodies towards mitigating users' privacy concerns, reducing user misconceptions, and assisting in users' adoption of privacy-protective behavior. We make recommendations accordingly.

2 Background & Related Work

Extended reality (XR) is an umbrella term for any technology that alters reality by adding digital elements to real-world environment to any extent and includes, augmented reality (AR), mixed reality (MR) and virtual reality (VR) [28]. While VR aims to separate the user from their real world and replace it with a digital world, AR overlays virtual objects into the real world, and MR combines both VR and AR [15]. Although all XR devices seamlessly integrate the virtual world with the real one through sensors, there are some significant differences between AR and VR when it comes to privacy.

Issues like bystander privacy are more pronounced in AR due to its always-on recording, especially in public environments [69], whereas VR provides a more immersive experience via extensive full-body tracking [23], synchronous voice chat and haptic feedback. Additionally, VR involves the use of avatars, virtual assets, friend-lists, and links to other social media [23], and requires privacy in user-interaction as well as content protection [31]. In this paper, we focus on the unique privacy challenges inherent to VR.

2.1 Privacy Risks

Many prior works have demonstrated the identification of users based on VR behavioral data including motion, bio-metrics, and usage patterns, with particularly high accuracy of identification when using machine learning techniques [38, 49, 65, 67, 68, 71, 91]. Certain VR software development kits and APIs allow access to sensors without explicit user permission, leading to privacy leakage [100]. Collected sensor data can not only be used to make inferences about physical/mental conditions, emotions and personality [12, 65], but further used to manipulate user behavior, such as purchasing decisions [64]. "Always on" VR devices enable constant surveillance, with greater possibility of inferences to be made about users [5].

2.2 User Concerns

Several studies have elicited user concerns in VR. One of the earlier works in this space by Adams et al. highlights user concerns centered around three aspects: well-being (including both physical well-being such as motion sickness and psychological well-being such as harassment), privacy, and to a lesser extent, security [5]. Regarding privacy, users are afraid of extensive data collection, especially from microphone and camera sensors [5]; the amount of concern correlates to what data they believe is being collected and how sensitive they consider that data to be [4].

Being a multi-user environment, VR brings the issue of multi-stakeholder privacy. When bystanders are present, users may accidentally share private information [21, 47]. While users have been found to be comfortable disclosing some types of information (e.g., emotions and personal experience) in social VR, they viewed disclosure as an inevitable trade-off [57]. Anonymity in VR, originally designed as a privacy mechanism, can also backfire as children are gaining access to VR platforms and exposed to mature situations (e.g., vulgar conversations) [56]. Another issue is deception and manipulation by increasingly realistic AI-generated faces, whom users have been found to trust more than real faces [12, 80].

2.3 User Practices

Despite these privacy concerns, users often share personal information with strangers in VR, finding VR communities to be exclusive and safe [5, 88]. VR often reduces social anxiety for users as it mimics social face-to-face interaction, while providing anonymity [5, 88]. One study of children found they enjoyed emotional connections and rich interactions in VR, though some risks existed [56]. Users disclose sensitive details about their lifestyle and sexuality in order to develop closer relations [88]. Their awareness of privacy risks in VR environments drops because of the gamified experience they perceive, leading them not to consider real-world consequences of their actions in VR [48]. Just as in other contexts, VR users have been found to accept terms and conditions of VR apps/platforms without reading them [39].

2.4 Privacy Mechanisms

Various privacy mechanisms have been recommended to address VR privacy implications, including VR-specific legislation that better protects the rights of users [70], adapting the permission models

from mobile platforms [46] and transparency for ad placements [80]. There are also technical proposals such as "incognito mode" where noise added to the user's telemetry data reduces the possibility of their deanonymization [66]. Interactive privacy tutorials based in VR have also been suggested to equip users with the knowledge to prevent doxxing (exposure of sensitive private information) or other forms of harassment [41, 50]. Features like embedded voice modulation [57] and privacy symbols [102] may also enhance VR privacy.

2.5 Comparison with Prior work

Our study is not the first to examine privacy in VR — prior work has elicited users' concerns around camera and infrared sensor data collection in VR systems [5] and self-disclosure in social VR [57]. However, the landscape may have changed in the past few years (e.g., Adams et al.'s work [5] was published in 2018), and VR has grown its user base from 15.6 to 32.7 million during this time [13]. With the rapid advancement of VR technology and its proliferation into professional use (fueled by the COVID-19 pandemic), such as apps for virtual desktops, our revisit of VR users' privacy concerns indeed yields new insights.

Adams et al. identified that users' privacy concerns primarily revolved around data collection, and privacy was secondary to physical and mental well-being [5]. Maloney et al. [57] mostly examined privacy concerns in the context of self-disclosure in social VR apps. While Hadan et al. [35] explore privacy perceptions of VR users, they investigate specific scenarios confined to single-user VR. Further, Cao et al. [14] study privacy concerns and behaviors of parents whose children use VR. By comparison, our study participants expressed privacy concerns along a wider range of dimensions — institutional, social, and device-related — and about new types of attacks, likely due to VR usage evolving and becoming more diverse. For example, participants raised concerns about digital replicas being created based on the pervasive forms of data collected in VR (e.g., voice, mannerisms, and avatars). They also highlighted the novel forms of 3D content creation facilitated by VR, and the challenges they pose around copyright and the confidentiality of intellectual property created in VR.

An emerging aspect of VR usage involves virtual desktops, when VR headsets are used to mirror another device. Our participants expressed concerns about using VR as a device to perform work-related tasks as it raises questions about the security of confidential information (since VR headsets have on-device chips and storage). However, some of our participants also mitigated these concerns by consulting the security team of their organization. We explored and identified many such privacy-protective practices of VR users. We also find gaps in users' expectations of VR data practices that make them underestimate the privacy risks in VR.

3 Methods

To identify users' privacy expectations, concerns, and consequently behavior, we conducted semi-structured interviews with 20 VR users. We present the study details below.[1]

3.1 Recruitment

We advertised our study on VR-specific subreddits (e.g., r/oculus, r/sidequest), Facebook groups, and Discord servers. We also used snowball sampling and asked the interviewed participants to advertise the study to their contacts. The study flyer included a link/QR code to a screening survey (see Appendix 7.1) for those interested in participating. In the screening survey, we asked about the frequency and duration of participants' VR usage, the headsets used, and the activities they performed in VR (e.g., socializing, playing games, and attending virtual events). We also asked them to specify their most frequently used VR apps via an open-ended question — the open-ended format intended to screen out participants who were not genuine VR users, who may otherwise randomly select provided answer options. We also collected demographic information including education level, gender, race, age range, and sexual orientation, to ensure participants' diversity, as participants from different under-served populations (e.g., women, racial/cultural minorities, LGBTQ+) may have different privacy needs and challenges [32, 36].

We received 125 valid responses from screening. A participant would qualify for the study if they were at least 18 years old, a resident of the United States, and currently used at least one VR application. In selecting whom to interview, we prioritized diversity in terms of the specific types of activities in VR and participant demographics to capture a wide range of experiences, concerns, and preferences. Based on these priorities, we invited 42 participants for interviews, of which 22 responded. Since online recruitment may lead to fraudulent participants [79, 90], as an additional verification that participants were indeed VR users, at the beginning of each interview, we asked the participants to turn on their webcam with their faces and VR headsets visible. We did not record the video when the participant's face was visible (this was specified in the consent form). The primary researcher was present for all the interviews and could ensure that no participant participated twice. Moreover, we asked a few questions specific to the participants' general usage of VR to gauge their level of familiarity with VR. Of the 22 participants interviewed, two did not present their VR headsets, and the researchers politely refused to proceed with the rest of the interview, resulting in a total of 20 *completed interviews*.[2]

Seven of our participants identified as women, one as non-binary; the rest identified as men. Nine were non-heterosexual, and six were from minority racial groups (see Table 3 in Appendix 7.2).

3.2 Interview Procedure

We conducted semi-structured interviews with the participants to qualitatively elicit their privacy expectations, concerns, and behaviors (Appendix 7.3 has the full protocol). Semi-structured interviews allowed us to elicit detailed perspectives from participants and ask follow-up questions when needed. We conducted virtual interviews to reach a larger pool of participants across diverse locations.

First, we asked participants about their usage of VR and the motivations behind usage. In probing about the usage, we asked participants about what/how data was collected and used by the VR apps (*expectation*). We particularly explored users' predicted privacy expectations [74] — "expected occurrence likelihood" [75],

[1] All study instruments are available at: **https://doi.org/10.17605/OSF.IO/PB3JE**

[2] One participant's camera was faulty; another participant was on vacation.

i.e., users' mental models of what they think happens [51], rather than aspirational privacy preferences. We next asked if they ran into any issues using VR, before probing into privacy-related concerns (*concern*). If concerns were brought up, we asked participants whether they had done anything to address them and why or why not (*behavior*). Throughout the interview, we asked participants to reflect on whether/how their concerns influenced their usage of VR and any specific features desired to address privacy concerns to make our findings more actionable.

Colnago et al. suggested that studying privacy constructs would be effective if participants were given specific descriptions of data practices [18]. As such, a significant portion of our interview revolved around a screenshot reaction activity. We presented information about data collection pertaining to the apps that the participants used through screenshots (Figure 5 in Appendix 7.4) and gauged their reactions. Although some participants used non-Meta headsets, we used screenshots from the Meta store for all participants for consistency, and because only the Meta store contained the detailed listing of privacy information among other VR app stores (SideQuest, App Lab, Steam). We provided screenshots for every VR app the participant listed that was also available on the Meta store. We showed participants screenshots of at least one app they used (min: 1, max: 7); in total, we showed screenshots of 36 distinct apps across all participants. To elicit participants' perceptions of privacy towards various VR platforms, we showed them an image containing branding of popular VR products (see Figure 2 in Appendix 7.4) and asked participants about their familiarity with the product and their expectations of the company's privacy practices.

3.3 Data Collection and Analysis

We hosted the screening survey using Qualtrics. Before conducting interviews with actual participants, we conducted five pilot interviews to assess the interview duration and refine the questions [54]. At the start of the interview, participants consented to participate in the study and be audio recorded. In interviews, when the researcher begins to hear the same comments again and again, data saturation is reached [81, 82]. We achieved data saturation [29] (i.e., additional interviews did not yield further insights) at the 18th interview. We conducted another two interviews to ensure saturation. Interviews were conducted in English via Zoom in July and August 2023. The average length of interviews was 43 minutes, and participants were given a 20 USD Amazon gift card upon completion of the interviews. The interviews were audio-recorded and transcribed using Whisper [73]. Two researchers conducted thematic analysis [11, 86] on the transcripts using deductive and inductive approaches. Deductive thematic analysis enabled coding based on Colnago et al.'s framework [18], while inductive coding was used to extract themes within the privacy constructs. The researchers coded two transcripts together to create the initial codebook. Next, they independently coded the rest of the transcripts in batches of four and discussed them to update the codebook. The two researchers discussed the codes and resolved any conflicts through several weekly meetings — an approach followed in several qualitative S&P studies [34, 37, 98]. Since every transcript was double-coded through discussions, checking intercoder reliability was not necessary [59].

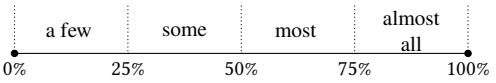


Figure 1: Terminology used to present relative frequency.

Since our study is qualitative with a small sample size, we refrain from reporting the exact number of participants associated with a given theme. However, to provide a sense of frequency, we adopt a consistent terminology shown in Figure 1 when reporting our qualitative findings.

3.4 Ethics

This study was approved by the IRB of all participating institutions. We carefully handled interview recordings and transcripts. We de-identified transcripts immediately after the interviews, deleted audio recordings as soon as possible, and stored all study data in a private repository accessible only to the researchers involved in the study. We also adopted trauma-informed interview practices — participants could skip any questions or quit the interview anytime without penalty [16, 99].

3.5 Limitations

The study relied on self-reported information from participants, which may be subject to social desirability bias. We recruited participants only from the US and from English-speaking forums. Recruiting participants from a broader range of cultural backgrounds and under served populations would address these limitations. When participants shared their privacy expectations, we did not correct their misconceptions (if any) during the study to avoid biasing them, especially if those required follow-up questions. Upon publication, we will share the paper, particularly our discussion on misconceptions (§5.3) with the participants. Although our results reflected that different populations have varying privacy needs (P3 reflected on their white male privileges in §4.2.4, and those who considered themselves "not being a target" were males), we did not find concerns associated with race/sexual orientation. With only 23% Americans owning a VR device [93], we acknowledge that our participants are likely to be skewed towards early-adopters of VR. Further, only three participants in our study used VR headsets for work-related tasks, limiting insights we could derive about this use-case of VR. Additionally, all of our participants used one of three handsets, with 13 being Meta Quest users, biasing our results to perspectives stemming from the use of these three VR devices.

4 Findings

Our participants used VR for a variety of purposes: a majority of them used VR for socializing and gaming, while many used VR for fitness-related activities and attending events in virtual spaces. Three participants used VR headsets to perform work-related tasks by connecting to a virtual desktop app, while one participant used visualization apps for his work in the field of architecture. At least four participants specified using VR for erotic role-play.

Participants' understanding of privacy in VR and consequently their concerns and protective practices arise from their exposure

to privacy-violating incidents as well as the privacy-related education they had. Several participants had encountered instances of doxxing, impersonation, and the recording and streaming of private interactions. Table 3 in Appendix 7.2 also contains details about the S&P education of the participants, which we asked participants about at the end of the interview. Three participants had formal education in S&P, through graduate degrees. Five participants reported having taken data S&P training as part of their work. Four participants explicitly mentioned that the only form of S&P training they had was about phishing scams. Eight participants had not received S&P-related education.

4.1 Users' Expectations of VR Privacy

Regarding VR users' *privacy expectations*, we find that participants expected a wide range of data to be collected (e.g., physiological data, and in-app interactions), for the purposes of delivering ads, generating revenue, improving user experiences and facilitating moderation. While these largely align with the technical realities, the vague terms in privacy policies and information leave participants speculating on the exact types and purposes of data collection.

4.1.1 Entities and Purposes Of Data Collection.

Participants expected that VR platform owners (e.g., Meta, Steam, Apple, etc.) and VR app developers would be the primary entities involved in data collection. They also believed third-party vendors, such as advertisers, may have access to collected data. P2 described:

> *"Usually developers of apps and websites collect information just to resell them to third parties." (P2)*

When questioned about the motives behind data collection, participants identified advertising and marketing, enhancing user engagement and app functionality, and content moderation as the main purposes for data collection. P16 speculated whether VR apps or platforms could monetize his data:

> *"The way your data would be processed, used, stored, permissions it would have on your system would be a concern. I'm paranoid, someone takes a scan of your face, could they monetize it?" (P16)*

We also asked about their perception of data collection in paid apps versus free apps. Participants had diverse views on this topic. Some believed free apps collected data primarily for ad serving and revenue generation. Regarding paid apps, while some thought they collected less data due to their payment model, a few participants believed they gathered as much data as free apps. P2 shared:

> *"If I'm paying for an app, I wouldn't want any of my data collected. But I know that that's not the way it is. If they can get extra money out of something they would." (P2)*

4.1.2 Data Types Collected.

Participants identified various types of data potentially collected during VR usage as summarized below.

Metadata about users. Participants perceived that their VR user profile, usage data, and analytics were utilized for enhancing apps through A/B testing. P16 felt usage data could be collected for recommending VR apps:

> *"Probably the same way most of the other information is used for internet usage . . . distilled down into profiles like, this person is into monster truck rallies and martial arts, maybe they'll be interested in this game." (P16)*

P16 also suspected that demographic information could be collected for the targeted development of VR apps, while P6 added that users' preferences and interests might lead to targeted advertising within or outside VR. P4 believed that metadata such as song preferences, playtime in VR, and types of people interacted with may be collected. P7 believed that the IP addresses of users need to be collected to impose an IP-based ban in the case of moderation.

Physiological data about users. A few participants specified that VR apps and platforms may collect physiological data. P3 shared that one of his fitness apps had his height and weight for calculating the calories burned. P10 added:

> *"I have full body tracking. You have to calibrate your height and trackers so they probably know about where these trackers sit on my body, my height." (P10)*

P11 felt biometric data like eye gaze may be collected:

> *"My face reaction to when they add a new feature . . . that would be used [for] advertising, seeing where you're looking, what you're clicking on, where you're going. I don't know if it is [happening] right now. Maybe it is." (P11)*

A few participants, such as P5, speculated whether developers had access to the feed of his personal living space:

> *"The manufacturer of the headset generally has access to motion data, and dimensions of your room that are scanned. Meta states that the developers have very limited or no access to that kind of data, but it's unclear what the manufacturers have access to." (P5)*

In-app interactions. Participants believed that their in-app conversations with other VR users could be monitored for moderation purposes. P11 explained:

> *"Every time you download a new app it says, we may be recording your audio. In Horizon Worlds if you are to get reported, they have the power to go back in time and watch what happens. They're recording my facial expressions, and I signed off to that." (P11)*

Some participants like P10 also noted that other VR users may be recording events and streaming them, and she would have no idea of such practices.

4.1.3 Understanding Data Practices.

When presented with screenshots of data collected by the VR apps they used, participants had varied reactions. In many cases, they believed the data collection was to be expected and rationalized based on the functionality of the app.

However, there were instances when participants could not identify a reasonable use case for a VR app collecting certain types of data. They used words such as "surprised", "interesting", "not sure" to describe their confusion:

> *"Interesting, now I'm curious about the other apps." (P2)*

P6 did not understand why "follower" information needed to be collected and speculated a potential use for it:

> *"I guess if someone has a ton of followers, they might share the game with others." (P6)*

Participants raised questions while trying to justify the collection of data, indicating a lack of clarity in the privacy information presented. P5 questioned:

"I don't necessarily know what data it's using via Bluetooth. Is it saying it needs Bluetooth in order to communicate with the controllers in some way? Because I don't know of any other way that a multiplayer video game would use Bluetooth on the headset. Do all applications that use the controllers also say Bluetooth? In which case, it's kind of a meaningless piece of data, right?" (P5)

While some participants could understand that microphone and storage was meant for facilitating in-app communication and storage respectively, others lacked awareness. P9 asked:

"VR chat says, microphone and storage, those are the two that pop out, so are [they] keeping audio recordings of people talking? And what's the storage mean?" (P9)

4.2 Users' Privacy Concerns

Regarding VR users' *privacy concerns*, we see that participants' concerns can be categorized into three types: institutional concerns (those directed to VR platforms/companies and regulators), social concerns (those related to other users or cross-platform inferences), and device-specific concerns (those enabled by specific device-related features and use cases in VR). These concerns are more extensive and cover a wider range of risks compared to prior work such as Adams et al. [5] and Maloney et al. [57]. Regarding the reasons for a lack of privacy concerns, some overlap with the reasons in non-VR contexts (e.g., "I've got nothing to hide" [83] and resignation [24]); others are unique to VR, such as the belief that VR devices are technically unfeasible to be "always on."

4.2.1 Institutional Privacy Concerns.

Platform and app surveillance. Some participants expressed their concerns with surveillance by VR platforms or individual apps, particularly when data collection happens without users' knowledge or consent. P1 expressed worries about potential recording or eavesdropping on VR conversations. P10 believed the moderation team in 'VRChat' had unrestricted access to join any instance, irrespective of its privacy settings being public or private. Additionally, P4 received a notification about a moderation bot entering a session while using VRCX [33] — a third-party friendship management tool for VRChat that alerts users about new session attendees — making them uncomfortable:

"I saw one of [VRChat's] moderation bots join our session and leave 10 minutes later . . . Having someone that's completely invisible, you can't see where they are, who they are, it's just there and then gone." (P4)

Some participants also shared their observation, and often resignation, that VR platforms and app developers had unrestricted access to all forms of usage data. P11 believed the app developers and Meta had access to everything she did. P16 expressed skepticism about the privacy of their VR interactions, assuming the data would "go through something" and it was not a peer-to-peer encoded communication.

A few participants' institutional concerns were further exacerbated by the possibility and prevalence of data breaches.

Sale and sharing of data. Some participants expressed how they were uncomfortable with their data being sold or shared. P6 was concerned about eye-tracking data being shared:

"Apple made a big point on their keynote with their Vision Pro to say that eye data isn't given to anybody. But there's a concern of it being like, "You have to watch this ad, if you're not, you can't continue." So I definitely think that information is valuable and could be passed along." (P6)

Some users expressed concerns about companies creating profiles of their users for targeted advertising. P9 suggested that companies developed "ghost versions" of users to deliver suitable ads. P7 expanded on this concern, noting its relevance not only to VR but also to general internet services. In contrast, P12 emphasized the diverse data collection capabilities in VR:

"It's not only your voice, or browsing history. They could store what you're doing, how you're moving, talking, the very core of what it means to be a human." (P12)

P9 further expressed concerns about the ethical use of AI-based data synthesis techniques in creating digital replicas of people, and how VR data may contribute to that:

"The technology is there to capture somebody's likeness. Somebody on Reddit was asking for legal repercussions because he was doing the narrating work for somebody, and they stopped paying and said, 'I don't need you anymore. I got AI to have your voice and do it for me."' (P9)

Lack of regulations. As the VR market becomes increasingly international, a few participants expressed their lack of trust in using VR products that are not heavily regulated in the US or are even out of the scope of US regulations. When asked about his perceptions about the privacy practices regarding Pico (a product of ByteDance, a Chinese company), P6 shared:

"People always say, 'Pick your poison. Do you want to give your data to Meta, an American company with different regulations that the United States government might have some control over, or do you want to get all your data to ByteDance which is a Chinese company.'" (P6)

P15 echoed these notions about using Pimax, a Chinese product, and believed that the company "had more leeway" in terms of data practices compared to US-based VR companies.

Influence of company size and reputation. Participants' institutional privacy concerns also diverge depending on the specific company involved. P16 compared several major VR headset manufacturers in terms of his level of trust:

"Microsoft is a huge corporation so I can never really know what's going on with them. Samsung is probably closer to Meta or Microsoft, because it's a huge multinational conglomerate with phones and other things." (P16)

The trust in the VR headset manufacturer also depends on the company's existing products and related surveillance. P12 explained why she would not use Microsoft's Hololens:

"Microsoft is the main OS I use. I don't know if I would feel comfortable sharing my conversations and movements, because they already have enough information." (P12)

Participants' lack of trust was sometimes rooted in the privacy-violating practices of companies that have come to light in the past, such as in the case of Meta. P1 shared:

"Meta might be recording the conversation. I don't know if I could trust them. MetaQuest is a new Facebook and we all know what they do on Facebook." (P1)

4.2.2 Social Privacy Concerns.

Eavesdropping and unauthorized recording by other users. Some participants talked about incidents when other VR users overheard private conversations not intended for them. P12 noted that one had to be careful while conversing in public worlds as others could be listening in:

"I was in a group with somebody I didn't know and mentioned the state I lived in. I saw them [a few] weeks later and they're like, oh, you're from that city and state." (P12)

Some participants, such as P2 and P10, expressed concern about their conversations being recorded and streamed by others. P9 and P12 highlighted concerns about being eavesdropped during VR activities involving drinking:

"If we've been drinking, we open up a lot. My best friends are on there. It's like you're sitting next to your friend. You don't want somebody listening into that." (P12)

A few participants also mentioned instances when users involved in ERP[3] had their private interactions recorded and shared by others. P10 shared one such incident:

"The person they were doing [ERP] with invited one of their friends over to the world they were doing it in. [Their avatar] could go completely invisible. They took pictures [and recordings] of the incident, shared it to a group chat jokingly. But someone started spreading it around." (P10)

While privacy violations between VR users can happen to anyone, P18 noted particular concerns about children's usage of VR and how they may give away information to predators.

Impersonation. While impersonation, the act of attempting to deceive someone by pretending they are another person, has been extensively studied in the context of social media [77, 105], our participants' sharing indicates that this particular attack has emerged in the VR space. P11 recounted how a VR user fabricated personal details when interacting with others:

"This girl pretended to be someone she wasn't. [A lot] of people knew [her] and one person found out that she was using photos that weren't hers and completely lying about every aspect of her life." (P11)

P18 had encountered many children in private instances that were meant for adults:

"There's worlds where your friends can freely join and where friends of your friends can join. It doesn't stop kids from being there if your friend has a kid friend." (P18)

P10 added that those who are hard-of-hearing or have a speech disability (who tend to interact via text) might have a higher chance of being impersonated, with a growing presence of people with disabilities in social VR [107]. She explained how they cannot use their voice to communicate if an imposter impersonated them by using their VR username:

"Let's say, they decide to change a certain in-game name without letting their friends know. If someone knew that they just changed it, they could immediately change their name to their old username and [act] as being the same person. You could [realize] after a certain period of time, but right away you could be fooled." (P10)

Doxxing. A few participants either experienced or witnessed incidents of doxxing. P13 described an incident when he was in a VR space and observed a user with details of another person (such as name, address, and personal details) floating above their avatar. P19 expressed that while most people would not be doxxed, it was "extremely scary" when it happened. Further, she highlighted how doxxing may be problematic for those with an online presence:

"If I were using my real name, I would be concerned about doxxing. People could search my name and find me easily. I work for a public organization so my contact info is public domain." (P19)

Cross-platform inferences. Some participants expressed concern about linking social media accounts to VR as it would reveal their personal information to others in VR. P15 shared:

"From my Facebook, people would literally know just who I am. It's real world information." (P15)

It was important to P18 that her interactions were not linked back to her employer. P11 expressed concerns about other users verifying the integrity of the personal information she shared about herself in VR:

"[My] one privacy concern is somebody channeling in on me and googling me to see if I'm telling the truth." (P11)

P16 further highlighted the potential for being tracked across virtual worlds based on profile information:

"If you had a persistent online handle and you were going from world to world, it'd be really easy to click follow and be pinged when that person was online." (P16)

4.2.3 Device-Related Concerns.

Leakage of confidential information. This concern is particularly relevant to those who use VR as a virtual desktop. A few participants, such as P6, who used apps to connect his work laptops on multiple screens in VR expressed concerns about apps being able to access confidential data:

"I am logged in on a work account, and if I'm using a headset, I'm wondering, is that data shared with the app I'm using [Immersed]? I'm not fully sure." (P6)

P20, a VR streamer, added that existing VR controls put them at risk of revealing her password while streaming:

"I wish devices and apps would have a quick button to stop streaming for 30 seconds. It's capturing my video. When I get a password entry prompt, I have to turn off the stream, enter my password, and turn it back on. People watching the stream might see a password entry screen. Even if it's censored out, they're gonna see those little circles and know how long my password is." (P20)

[3]ERP, or Erotic Roleplay, is a form of sexual online roleplay performed through online video games, chatrooms, forums, etc. [22]

Access to sensory data. Some participants expressed concerns about VR devices' potential access to sensor data. P4 felt uncomfortable having many cameras and microphones, a concern he also shared about IoT and mobile devices. P3 believed user discretion was critical in ensuring that images recorded by the device would not capture anything sensitive:

"Most of the new devices use camera-based tracking and, whether the terms of service says it's not gonna happen or not, images are recorded by the device." (P3)

Similarly, P12 expressed her distrust in on-device processors and untethered ("mobile") VR headsets:

"There are two types of VR, PC VR and mobile VR. A big reason why I didn't want to go with MetaQuest is they have mobile VR. The chipset in their headsets is [like] that of an iPhone. The PC VR uses your computer's processor by plugging directly into that. All the downsides outweighed the benefits of it being mobile." (P12)

4.2.4 Reasons for Lacking Privacy Concerns.

Awareness of data practices. A few participants who had technical knowledge about VR systems could explain why certain types of data collection were not technically feasible and thus expressed a lack of concern towards them. P19 was less concerned about VR headsets collecting sensitive environmental data as they were not "always on":

"Unlike phones, Alexa or Google Home, your headset isn't on all the time. 90% of the day, it is off and sitting on the ground, not like it's tracking your location." (P19)

Similarly, P3 linked his understanding of the Android OS to his trust in his Android-based Meta Quest device:

"Android is protecting me from application developers, what level of data they can gather. To record the screen or access the microphone, it has to ask me permission." (P3)

A few participants also consulted certain sources — such as privacy policies — to develop their knowledge of data practices in VR. The transparency of OpenXR, an open-source standard for VR platforms, mitigated certain concerns for P4, as he could verify what sensor data was accessed or used.

Further, there are features in VR apps that help raise participants' awareness of data collection. P8 described how some private worlds were invite-only and did not pose concerns of unauthorized recording by bystanders. P4 explained:

"Neos puts a thing above your head that says 'live'. In VR chat, you can see when people have cameras out." (P4)

Willingness to share data to improve VR experiences. A few participants expressed their lack of concern about data collection when they believed the collected data could be used to improve their VR experiences. P4 shared:

"It might be useful for the team to know how many people use full body tracking because that can help them focus their efforts on what is relevant to most users." (P4)

P6 wanted VR to "continue and succeed" and was happy to share eye tracking and facial recognition data as he wanted to indicate to the developers that he liked the particular feature and wanted them to continue improving it. The value of great VR experiences can sometimes even outweigh concerns related to sensitive information. A few participants, such as P4, were not concerned about the collection of health-related information as long as it was relevant to the app functionality.

The same exception can also made for specific purposes for which the data is used. P6 felt the benefits of data collection for content moderation outweighed the privacy risks:

"If someone is saying disrespectful things, it has to be tied back to [them] so something can be done to keep them from making the social environment negative. Having that data, even if it is tied to me, my microphone and actions, makes a better social experience for everybody. The benefits of that outweigh the negatives." (P6)

Users' trust in various entities. A few participants attributed their lack of concern to their trust in the users they interacted with on VR. P4 only interacted with known users in VR and did not mind if they recorded anything. He further trusted the VR app, 'Neos', and its welcoming user community:

"As a new user of Neos, I was approached by people incredibly willing to help me. Knowing the creator of Neos, I know how things are being handled. So I feel a lot more comfortable." (P4)

P3 trusted Valve and Steam as they did not have an ad network. P12 explained that she trusted VRChat, due to their economic infeasibility for massive data collection:

"I trust VRChat as a company and know they're a small startup. The way their servers are always breaking down, I don't believe they'd be able to afford the storage to record every single person using that game." (P12)

P18 believed in the notion of "higher price, better privacy" and thus trusted Apple's products:

"With the price comes this idea of high quality, good fidelity in terms of privacy. To my knowledge, [Apple] don't share a lot of information with other companies." (P18)

Lack of perceived harms. Most participants described situations where they believed data was collected about them yet did not have any concerns, due to their inability to identify reasonable use cases or potential harms of its use. P1 shared:

"Even if they knew all of my usage data on the Quest device, what are they gonna do with it?" (P1)

The lack of perceived harm even applies to more sensitive data types. P14, who self-identified as having autism, did not mind VR apps inferring that they had a health condition. About physiological data collection, P15 shared:

"If someone knows how tall I am and how I move, I don't think there's anything they can do with that data." (P15)

Solove [83] identified "I've got nothing to hide" as a common reason for justifying a lack of privacy concerns; yet it is a misunderstanding, as privacy has broader social values and is more than hiding one's secret. This notion was also present among our participants. A few believed that their interactions in VR did not reveal anything controversial about themselves. P11 shared that she was an "open book" and did not do anything "weird" in VR. P6 felt that microphone data collection could be a concern only if users were being disrespectful:

"If I'm with strangers I'm not conducting myself any differently than I would with a stranger in the real world. So if that information is shared, I'm not concerned." (P6)

People may be overconfident in their assessment of privacy or security risks, a phenomenon known as optimism bias [3]. Along this line, almost all participants attributed their lack of concern to their belief that they were not a "target." P9 described himself as "a number" in the system. P3 felt minorities are more likely to be targeted:

"I am privileged enough to be a white male ... If I was trans, homosexual or had things that I had been oppressed for, I would want to keep that information private." (P3)

A few participants expressed resignation [24] about data collection because they believed the collected data was already available to companies or in public through other means. P10 believed that nothing she did on the Internet was private and did not mind if any entity learned more information about her. P16 added:

"The ship has sailed on data privacy in a lot of ways. I'm not super concerned about someone knowing that I'm a [age] old guy that watches a lot of anime. It seems like there isn't a way for someone to participate in a lot of these things without making that concession." (P16)

4.3 Privacy-protective Usage of VR

Regarding VR users' *privacy practices*, we find that participants undertook various *device-oriented*, *app-oriented*, and *interaction-oriented* measures to protect their privacy.

4.3.1 Device-Oriented Measures.

Purchase "privacy-friendly" VR headsets. Users' intentional consideration and purchase of "privacy-friendly" VR headsets emerged to be a key device-oriented measure, although they largely relied on heuristics rather than in-depth analysis. One heuristic is the reputation of the VR headset manufacturer. A few participants shared that they purchased non-Meta headsets as they did not trust the company's privacy practices. P13 switched from an Oculus to a Valve Index:

"I decided to switch to a Valve Index which is owned by Steam and has more privacy compared to Meta." (P13)

P19, while aware that Meta had no privacy-related incidents related to VR, still did not consider purchasing Meta headsets:

"The ones created by Meta were out of the running right away. I don't use Facebook or Instagram for lots of reasons, but one of the concerns is privacy. It wasn't about privacy regarding the headset, but I don't want to give money to a company that does that kind of thing." (P19)

Even among participants who purchased Meta's headsets, there was distrust in Meta's privacy practices. P5 shared that because he owned a Meta headset, he was more conscious while using it, and that it impacted his VR usage.

Where the VR headset was manufactured was another heuristic. Participants reported switching from headsets manufactured by non-US companies to US-based ones. For instance, P6 switched from Pico to the Meta Quest.

Minimizing device access to sensitive data. In cases where their headsets had dedicated storage and on-device processors, a few users specified not storing sensitive data on-device:

"I don't have any private information on the storage of my Quest, because some apps may have access to it." (P1)

P6 described his conscious effort to ensure he did not have sensitive things in the environment while using VR.

Upgrading to newer VR devices. P1 believed in the notion of "new device, better security" and shared how upgrading to newer VR devices came with higher security guarantees:

"The newer devices might receive the latest security updates. That might add privacy features and make your device to be less likely to be compromised." (P1)

4.3.2 App-Oriented Measures.

Checking data practices before app use. Some participants looked for app-specific information, such as obvious issues with the app, through comments on online forums. P2 shared:

"I usually read a few comments. If an app had some problems, there would definitely be some comments online or on the Oculus app that would tell a cautionary tale." (P2)

P3 looked for complaints about data leakage, while P6 watched videos of others using a VR app prior to his usage:

"I watch videos of people using the app. If something is new, and untested by others, I'd be unlikely to use it." (P6)

Some users also checked the app's data sharing, storage, and usage practices. P4 read the privacy policies for untrusted apps. P1 detailed the factors he weighed during sign-up:

"What do they want to know before allowing me to use the app? How do they want me to register to use the app? How are they going to verify my information?" (P1)

Minimizing cross-platform inferences. Beyond checking specific information prior to use, participants also described personal rules they followed while using apps. Some participants such as P15 did not link their social media accounts to VR and created a new one for VR usage:

"When I set it up, I made a new email to create my Oculus account so that wouldn't be tied to anything else. They forced a Facebook login [for a while]. I didn't do that and waited for the Meta login to come and switched." (P15)

Minimizing access to sensitive data. An example along this line is ensuring that the usage did not violate confidentiality, particularly when VR is used for professional work. Two out of the three participants who used VR for work obtained permission from their workplace. P3 shared:

"I had our security folks check out 'Immersed' and they're okay with the way it acts as a remote desktop client." (P3)

P19 was conscious about sharing any information that may be problematic in the event of a data breach:

"I'm not giving away anything that I am not comfortable with leaking if they have a data breach." (P19)

P1 granted permissions based on the app's functionality:

"When you first start an app, it asks for certain privacy settings, like accessing the photos on your device. I would generally deny that. But if it's an app where you're chatting with people, I would allow microphone access." (P1)

P7 described using a VPN assuming it would deter advertisers from utilizing data gathered from VR apps:

"VPN is definitely the best option right now because it encrypts your personal data so advertisement companies can't easily look at your information. It's gone through so many things that it's basically useless to them." (P7)

4.3.3 Interaction-Oriented Measures.

Avoiding the disclosure of personally identifiable information. Almost all participants specified that they did not share their personally identifiable information (PII) such as name, workplace, or contact information. Some shared their names if they believed it was a common name; otherwise, they used a pseudonym and shared their city if it was a populous one. If they wanted to communicate more with users they met in VR, they shared other social media details (such as WhatsApp, Telegram, and Discord) to continue non-VR-based communication. Participants noted that they preferred not to share their phone numbers with users in VR. P1 explained:

"If I'm talking with someone, usually I wouldn't give any personally identifiable information. I would go by a username. I might tell them where I live. If I live in New York, I would tell them that because a lot of people live in New York City, so I don't care that much about that. I try to keep things private so that if there is someone that tries to find me, hopefully they won't be able to. But if there are specific people, if I trust them enough, maybe I would give them my phone number. And then I could like chat with them on WhatsApp or a discord." (P1)

Limiting certain types of interactions. Many participants reported limiting their interaction in public virtual spaces and described socializing like they would in real life. P3 shared:

"When I use something like VRChat, I assume that the administrators know everything I do within that. I modulate my activities, assuming it's a public space." (P3)

Participants also mentioned using only single-player apps or not engaging in private activities such as ERP in VR. The reasons for these heuristics stemmed both from their expectations of privacy in VR and their general personal preferences. P3 stayed away from multiplayer games with strangers as he did not want others observing him. P5 added:

"I'm [mostly] using single-player experiences where I'm not generating any sensitive data I'm concerned about. I'm not having communications I consider private." (P5)

Some users such as P4 switched to more trusted apps for certain interactions, such as spending time with his partner:

"I don't usually interact on VRChat. I usually go on Neos. I know the person who created Neos. So I know for a fact that nobody's going to be snooping." (P4)

4.3.4 Reasons for Lacking Protective Measures.

While protective behaviors exist, participants mentioned behaviors that would invariably increase their exposure to privacy risks. Most participants admitted that they did not read the terms of service, license agreements, or privacy policies of VR apps, a known phenomenon also found in users' interactions with websites and mobile apps [58, 85]. A few participants acknowledged that they did not pay attention to the permissions they were granting to VR apps. We next elaborate on the reasons why participants sometimes consciously avoided privacy-protective measures in VR.

Limited concern and awareness of privacy implications. In some cases, the lack of privacy-protective practices was aligned with a similar lack of privacy concerns. For instance, P6 believed that data collection improved his VR experience, and consequently, he did not adopt several privacy-protective practices. Some participants, such as P18, admitted that she did not consider the data practices of the apps she used and their privacy implications:

"I will switch over to [my] virtual desktop and you could potentially see my Discord stuff. I wouldn't call that super sensitive, but is it private? Yeah, totally." (P18)

P2, who used "Arkio", a 3D visualization app for architectural work, admitted that he did not know whether "Arkio" could access his 3D visualization work data from the app:

"We come across so many privacy agreements, we are inclined to just accept it. I have no idea if a third party could access my information, or if I agreed to it." (P2)

Interestingly, P5 was aware of research on the privacy risks related to inferences based on VR data [67], but commented that the awareness was not enough to motivate behavior:

"I've seen studies where, with a small sample of people, they could identify an individual within five seconds, just based on their head and hand movements. It's something I think about, but doesn't prevent me from using VR." (P5)

Desire to continue enjoying VR. If a VR app was enjoyable, participants continued using the app without worrying about privacy. P13 shared that he had never stopped using an app or uninstalled an app due to privacy concerns. P4 added:

"It's mildly embarrassing, but I usually continue to use the app … what am I going to do, make my own?" (P4)

The act of agreeing to privacy-violating terms for the sake of using an app was shared by most participants. P10 said:

"I'm not going to take an experience away from myself because my information that's already being sold to third parties is all continuing to be sold to third parties." (P10)

Economic considerations in switching VR headsets. Participants' distrust of headset manufacturers did not deter continued usage, mainly due to the headset's cost. P18, a Meta Quest user who expressed concerns about Meta, shared:

"The Index, the other well-known high-quality headset, costs $1,000. Quest costs a few hundred." (P18)

P15 highlighted the difficulties in switching VR platforms:

"Prices of Oculus and PlayStation at the time [of purchase] was $300 and $900. It was a pretty big price difference. Also [now] I have all my games bought through Oculus so I wouldn't really be able to switch." (P15)

	Subtype	Name	This work	AR/VR [35]	[5]	[57]	[47]	[30]	[2]	[69]	[14]	IoT [108]	[106]	[89]	[45]	Smartphone [17]	[42]	[43]	[72]	Social Media [84]	[53]	[44]	[97]
Institutional Privacy Concerns	Platform/app surveillance	Recording conversations	●	–	–	–	–	●	●	–	–	–	●	●	●	–	–	–	–	–	–	–	–
		Eavesdropping for moderation	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		Unrestricted/unauthorized access to (usage) data	●	–	–	–	–	–	●	–	–	●	●	●	–	–	–	–	●	●	–	–	–
	Sale/sharing of data	Eye-tracking data	●	●	–	–	●	●	●	–	●	–	–	–	–	–	–	–	–	–	–	–	–
		Profiling for targeted ads	●	–	–	–	●	–	●	–	●	●	●	●	●	–	●	–	●	–	–	–	–
		User gait	●	●	–	–	–	–	●	●	–	–	–	–	–	–	–	–	–	–	–	–	–
		User speech and style	●	●	–	–	–	●	●	●	●	–	●	–	●	–	–	–	–	–	–	–	–
		User interests	●	●	–	–	●	–	●	●	●	–	●	●	–	–	–	–	–	–	–	–	–
		AI-based digital replicas	●	–	–	–	–	●	●	●	–	–	–	–	–	–	–	–	–	–	–	–	–
	Regulations	Distrust in non-US companies	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	Company size/ reputation	Distrust in large corporations	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		Surveillance through company's various products	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		Distrust based on previous data breaches/approach towards privacy	●	–	●	–	–	–	–	–	–	–	–	–	●	–	–	–	–	–	–	–	–
Social Privacy Concerns	Recording by other users	Eavesdropping on conversations/social activity	●	–	–	–	–	●	–	–	–	–	●	–	–	–	–	–	–	–	●	–	–
		Live streaming of VR sessions by bystanders	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		Recording of intimate activities (ERP sessions)	●	–	–	–	–	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		Eavesdropping during drinking-based activities	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		Risky disclosures by child users	●	–	–	–	–	–	–	–	●	–	–	–	–	–	–	–	–	–	–	–	–
	Impersonation	Fabricating personal information while interacting	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		Children posing as adults	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		Impersonation of hard-of-hearing individuals	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	Doxxing	Doxxing of users whose identity is public	●	–	–	–	●	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	Cross-platform inferences	Linking social media to VR	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		Interactions/ activities reaching employer	●	–	–	–	–	●	–	–	–	–	–	–	–	–	–	–	–	–	●	●	–
		Digital stalking of a user after interacting with them in VR	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Device-related	Confidential info leakage	Info leakage while using VR as virtual desktop	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		Leakage of password length while livestraeming	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	Access to sensory data	Surroundings/bystanders captured by cameras	●	●	●	–	●	●	●	●	–	–	–	●	–	–	–	–	–	–	–	–	–
		Leakage/misuse of audio recorded by microphones	●	–	●	–	–	●	–	●	–	–	–	●	●	–	–	–	–	–	–	–	–
		Distrust in untethered/ standalone devices	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

Table 1: Privacy concerns across contexts. (● privacy concern identified in cited work; – privacy concern not identified in cited work)

5 Discussion

5.1 Privacy in VR vs. Other Contexts

Our findings highlight a wide range of users' privacy concerns — institutional, social, and device-related — compared to prior work on VR privacy [5, 57]. Beyond prior work in VR, it is important to situate our findings in prior work on privacy concerns and behaviors in other contexts to better understand to what extent these findings are uniquely associated with VR (we exclude privacy expectations from our comparison because fundamental data practices, context-specific privacy education, and other factors vary by platform). For instance, existing work shows that reviews and brands are the primary considerations when users install mobile apps [17], and features and price are the primary considerations when users purchase IoT devices [108]. Our findings show similar trends in participants' behaviors when installing VR apps or purchasing VR headsets. AR users have expressed concerns about eye tracking and the potential sharing of such data to advertisers [30], similar to our findings about VR users. However, there are also notable differences between users' privacy concerns and behaviors in VR versus other contexts. In Tables 1 and 2, we compare the privacy concerns and privacy-protective behaviors uncovered in this work with those reported by prior academic works studying user privacy perceptions across multiple platforms, including AR/VR. We identify **14** unique privacy concerns and **eight** unique privacy-protective practices (highlighted in grey in the figures). While we report all the privacy concerns and privacy protective-practices mentioned by our study participants, we also note that some of these concerns or practices may be misplaced, due to misconceptions of the participants. We discuss this further in §5.3.

5.1.1 *Limited concerns about "always on."*

Prior work has highlighted user privacy concerns over "always on" devices such as smartphones [40], smart speakers [55] and AR glasses [30]. By comparison, VR devices do not have this "always on" feature and typically do not travel with the user. This might also explain why, among our participants, few had salient concerns about location privacy. Interestingly, "always on" microphone/camera data collection was a prominent privacy concern highlighted by Adams et al. [5]. A possible explanation for this difference is, as VR gains adoption, users are more familiar with the capabilities of VR.

5.1.2 *Users largely aware of biometric data collection.*

VR is unique in its ability to gather and process a rich set of biometric data, including motion and interaction tracking. The camera-based tracking enabled by VR headsets poses concerns to the users, as the camera may capture sensitive information about their physical environment. Most participants exhibit awareness about biometric data collection, with a few (P9 and P12 in §4.2.1) sharing concerns. While many institutional concerns regarding surveillance and unauthorized data sharing pervade platforms (Table 1), we uncover concerns related to the size of the device manufacturers.

5.1.3 *VR content moderation leading to privacy infringement.*

VR experiences — particularly social VR — often involve content moderation. While traditional social media platforms involve textual or image-based identification [60, 103] of inappropriate content [61, 62], in VR, moderation is done manually by developers/moderators or semi-automatically, by involving third-party

	Subtype	Name	This work	AR/VR [35]	[5]	[57]	[47]	[30]	[2]	[69]	[14]	IoT [108]	[106]	[89]	[45]	Smartphone [17]	[42]	[43]	[72]	Social Media [84]	[53]	[44]	[97]
Device-oriented	"Privacy-friendly" devices	Buying device from company whose privacy practices user trusts	●	●	–	–	–	–	–	–	–	●	–	–	–	–	–	–	–	–	–	–	–
		Conscious usage if lacking trust in manufacturer	●	●	–	–	–	–	–	–	–	–	–	●	–	–	–	–	–	–	–	–	–
		Switching to US-based manufacturers	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	Data access	Not storing sensitive data on-device	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	●	–	–	–	–	–
		Not having sensitive things in environment	●	●	–	–	–	●	–	–	–	–	●	–	–	–	–	–	–	–	–	–	–
	Upgrades	Upgrading to devices with greater security	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
App-oriented	Check before app use	Check for reviews / comments on online forums	●	●	–	–	–	–	–	–	–	●	–	–	–	●	–	–	–	–	–	–	–
		Watch videos of app use before installation	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		Check app's data sharing, storage, usage practice	●	●	–	–	–	–	–	–	–	–	–	–	–	●	–	–	–	–	–	–	–
		Reading app's privacy policy	●	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	Cross-platform inferences	Not linking social media account to VR	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		Limiting personal information disclosed to VR platform (creating new email for VR)	●	–	–	–	–	–	–	–	–	–	–	●	–	●	●	●	–	●	–	–	–
	Minimzing access to sensitive data	Obtain permission from security team of workplace before using VR for professional work	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		Not sharing sensitive information	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	●	●
		Grant permission based on core app function	●	–	–	–	–	–	–	–	–	–	–	–	–	–	●	●	–	–	–	–	–
		Using VPN	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Interaction-oriented	Avoiding disclosure of PII	Not sharing PII such as name, workplace or contact information	●	–	–	●	–	–	–	–	–	–	–	–	–	–	●	–	–	●	–	–	–
		Using pseudonym	●	–	–	●	–	–	–	–	–	–	–	–	–	–	–	–	–	●	–	–	–
		Private conversations (using non-VR based communication)	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	●	–
	Limiting certain types of interactions	Socializing like in real life	●	–	–	–	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		Avoiding certain functionalities (using only single-player apps)	●	–	–	–	–	–	–	–	–	–	–	●	–	–	●	●	–	–	–	–	–
		Not engaging in private activities such as ERP	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		Not engaging with strangers	●	–	–	●	–	–	–	–	–	–	–	–	–	–	–	–	–	–	●	●	–
		Use trusted apps for private interactions	●	–	–	–	–	–	–	–	–	–	–	–	–	●	–	–	–	–	–	–	–

Table 2: Privacy-protective behaviors across contexts. (● privacy behavior identified in cited work; – privacy behavior not identified in cited work)

entities [76]. This aspect of VR can adversely create an impression of privacy infringement due to the lack of transparency in the presence of moderators, as highlighted by P4 in §4.2.1.

5.1.4 Bystanders as potential adversaries.

We identify seven social privacy concerns distinct from other contexts and AR/VR such as livestreaming of VR sessions by bystanders and digital stalking of users after VR-interaction. Our participants (e.g., P9, P12, P14) expressed concerns about recording and sharing interactions while engaging in VR activities involving drinking and ERP (§4.2.2). In this way, VR increases the chances of unintended information disclosure and the consequent doxxing compared to other technologies. Impersonation can also increase the potential for scamming and other social engineering attacks in VR, particularly to users from vulnerable populations (e.g., hard-of-hearing individuals, children). We identify concerns of information leakage while livestreaming VR sessions and using VR as virtual desktops.

5.1.5 Privacy-protective behavior adopted from other contexts.

Our participants shared 13 strategies previously unreported in the literature for VR privacy protection, such as obtaining permission from security team before using VR for work, not engaging in private activities, and using trusted VR apps for private conversations. However, an analysis across contexts reveals that privacy behavior for VR is largely adopted from those of IoT, smartphone, and social media. While device-oriented measures largely align with those for IoT, app-oriented measures match closely with privacy-protective strategies for smartphone. Interaction-oriented measures include a combination used for IoT, smartphones and social media.

5.2 Privacy Expectations vs. Reality

As illustrative examples, we outline the practices of Meta (a VR platform) and VRChat (a VR app) to compare users' expectations with technical realities. Meta claims to collect user profile (e.g., username, avatar, list of followers), VR product activity (e.g., VR events attended, duration of VR usage), and fitness information (e.g., calories burned). Hand and body tracking, eye tracking, facial expressions, and surroundings image data are collected, however, their raw data is processed on device [63]. VRChat collects usage, as well as body and movement information (if enabled) [96]. They specify that they do not collect or scan retinas to gather eye data. The collected data is stated to be used for analytics and advertising, securing the platform, communicating with the user, and for research. These practices largely align with most participants' expectations.

For moderating "Horizon Worlds" (a VR app by Meta), Meta states that the last few minutes of a users' most recent audio, video and other interactions in Horizon Worlds are recorded and stored on their server [63]. VRChat, in contrast, states that they may record audio and video for limited situations. However, contrary to many of our participants' expectations (such as P12 in §4.2.4), they may record even in private instances [95].

The Meta store includes an "app privacy" section detailing the sensors, device data, requested by app developers (Figure 5 in Appendix 7.4). Steam and PlayStation stores provide the interaction and hardware feature details, but not privacy-specific information (Figures 3, 4 in Appendix 7.4). While Meta's approach is a good step towards transparency, §4.1.3 highlights the downsides of providing vague information that triggers incorrect understanding among users. More efforts can be directed to evaluating and improving

such "privacy labels" for VR apps, similar to mobile app [20] and IoT privacy labels [26]. In particular, misconceptions need to be addressed when they lead to an underestimation of privacy risks.

5.3 Practical Implications

Our findings have practical implications for researchers, VR developers and designers, and regulators, which we discuss as follows.

5.3.1 Reducing user misconceptions.
Participants such as P1 in §4.2.4, exhibited a lack of awareness about the implications of biometric data collection as they commented *"What are they gonna do with my data?"*. Similarly, P3 wondered if any data leaks actually cause harm. Nair et al. [68] showed that recordings of a target's movement data can be used to identify the ethnicity, income, physical/mental disabilities, and use of substances with more than 50% accuracy. Not only can these attributes be used by platforms or apps to serve personalized ads, they may also be shared with insurance companies or exploited by repressive governments. VR users should be informed about the harms that can arise from these inferences, including price discrimination, and pushing political agendas [31]. Researchers have uncovered ways in which an adversarial VR user can extract sensitive information of other VR users such as financial data and passwords through keystroke inference attacks [101] and remote keylogging attacks [87].

A few participants expressed a misplaced concern based on the perceived lack of regulations on non-US based VR products (§4.2.1). However, privacy regulations such as General Data Protection Regulation (GDPR) [19] and California Consumer Privacy Act (CCPA) [9] are applicable in various jurisdictions irrespective of country of origin of the company. Because all of our participants were US residents, it is possible that some of them lacked knowledge on regulations in other jurisdictions.

P7 shared their usage of a VPN for protecting their privacy (§4.3.2) during VR usage. While VPNs may protect from network adversaries, they are not applicable against the hardware, client, server, or user adversaries identified for VR [31].

Recommendation 1: Privacy-focused onboarding tutorials [57] should be provided to users by VR app developers and VR platform owners. Social media outreach [1, 104] regarding VR privacy may be designed by privacy educators for the VR community to enhance user awareness.

5.3.2 Mitigating users' privacy concerns.
It is important to mitigate users' privacy concerns for the following reasons: (i) incorrect concerns may impact users' trust towards the manufacturers and their intention to continue using the devices, (ii) their concerns may also impact their experiences when using the devices. However, in other cases, users' concerns might be valid; this is when companies should improve their data practices by adopting user-desired, privacy-friendly data practices. The data practices desired by some participants already aligned with guidelines in GDPR [19], such as collecting only necessary data (data minimization in Art. 5), storing data for a reasonable amount of time (Art. 17 about 'the right to be forgotten'), and being transparent about data collection (Art. 7 about consent). Nonetheless, it remains unknown to what extent VR apps comply with existing regulations, compared to the large body of auditing research on mobile apps [7, 78] and consent notices [10, 92].

Recommendation 2: More third-party auditing on VR apps' and platforms' compliance with regulations could lead to enforcement of better data practices that take the burden of self-protection from end-users.

Within the notice and choice framework, another avenue of intervention is in-app and system-wide privacy features that enable VR users to have more granular control over the specific types of data collected, the ability to view and delete previously collected data, and features similar to "ad blockers" or "private browsing mode" in VR. Participants also desired alternative versions of VR apps that had limited functionality but better privacy protection so that they could still use the app for its basic features even if they opted out of data collection. Specific obfuscation features could be developed to deal with P20's case, where password length was being observed by their streaming viewers (§4.2.3).

Recommendation 3: Privacy researchers and VR app developers should develop privacy-preserving techniques and integrate them into VR systems for users to exercise fine-grained privacy controls.

5.3.3 Assisting users in adopting privacy-protective behavior.
Since VR has not reached its technological maturity, the starting price of the device is naturally the primary factor influencing users' purchase decisions and overrides privacy considerations, as shown by our findings (§4.3.4). An interesting direction to explore is how much users are willing to pay for VR privacy, similar to IoT [27]. However, unlike IoT devices, which have a multitude of products at various price points, VR is driven by a few major players.

Recommendation 4: Action by regulatory bodies is needed to drive the diversification of the VR market, particularly enforcing that privacy-friendly solutions be offered for a correct price and providing consumers with more choice for their privacy.

6 Conclusion

In this paper, we report on the findings from interviews with 20 VR users about their privacy expectations and concerns based on their VR usage and the corresponding privacy-protective practices they adopt. Participants express institutional, social, and device-related privacy concerns, which they mitigate by privacy-friendly device selection and selective engagement in VR interactions, among others. They also reveal misconceptions in their understanding and implications of VR data collection. With the VR ecosystem burgeoning, the collaboration among VR platforms, app developers, regulators, and researchers is critical to address VR user privacy.

Acknowledgments

We are deeply grateful to our participants. We extend our thanks to Alex Ross, Greg Tystahl, Ramzah Rehman, Seaver Thorn, and Virgil English for their feedback on the interview protocol. We also thank our anonymous reviewers for their valuable feedback. This research is partially supported by a Meta Research Award on 'People's Expectations and Experiences with Digital Privacy,' the National

Science Foundation (NSF) under grants CNS-2350075, CNS-2341187, IIS-2328183, the Max Planck Society, and the Deutsche Forschungsgemeinschaft (DFG) under Germany's Excellence Strategy - EXC 2092 CASA – 390781972. The opinions, findings, conclusions, or recommendations expressed in this work are those of the authors and do not necessarily reflect the views of the funding organizations.

References

[1] Jemal Abawajy. 2014. User preference of cyber security awareness delivery methods. In *Behaviour & Information Technology*, Vol. 33. Taylor & Francis, 237–248.

[2] Melvin Abraham, Pejman Saeghe, Mark Mcgill, and Mohamed Khamis. 2022. Implications of xr on privacy, security and behaviour: Insights from experts. In *Nordic Human-Computer Interaction Conference*. ACM, 1–12.

[3] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, et al. 2017. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)* 50, 3, 1–41.

[4] Devon Adams, Alseny Bah, Catherine Barwulor, Nureli Musabay, Kadeem Pitkin, and Elissa Redmiles. 2018. Perceptions of the privacy and security of virtual reality. In *iConference 2018 Proceedings*. iSchools.

[5] 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.

[6] Abrar Alismail, Esra Altulaihan, MM Hafizur Rahman, and Abu Sufian. 2022. A systematic literature review on cybersecurity threats of virtual reality (VR) and augmented reality (AR). *Data Intelligence and Cognitive Informatics: Proceedings of ICDICI 2022*, 761–774.

[7] Noura Alomar and Serge Egelman. 2022. Developers say the darnedest things: Privacy compliance processes followed by developers of child-directed apps. *Proceedings on Privacy Enhancing Technologies* 4, 2022, 24.

[8] Thomas Alsop. 2023. Virtual reality (VR) - statistics & facts. https://www.statista.com/topics/2532/virtual-reality-vr/#editorsPicks

[9] Rob Bonta. 2023. GCalifornia Consumer Privacy Act (CCPA). https://oag.ca.gov/privacy/ccpa

[10] Ahmed Bouhoula, Karel Kubicek, Amit Zac, Carlos Cotrini, and David Basin. 2023. Automated, Large-Scale Analysis of Cookie Notice Compliance. In *USENIX Security Symposium*.

[11] Richard E Boyatzis. 1998. *Transforming qualitative information: Thematic analysis and code development*. sage.

[12] Lauren Buck and Rachel McDonnell. 2022. Security and privacy in the metaverse: The threat of the digital human. *CHI EA*.

[13] Stefan Campbell. 2023. How Many People Use VR in 2023? (Virtual Reality Stats). https://thesmallbusinessblog.net/how-many-people-use-vr/

[14] J. Cao, A. S.B., A. Das, and P. Emami-Naeini. 2024. Understanding Parents' Perceptions and Practices Toward Children's Security and Privacy in Virtual Reality. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, Los Alamitos, CA, USA, 229–229. https://doi.org/10.1109/SP54263.2024.00182

[15] Derin Cayir, Abbas Acar, Riccardo Lazzeretti, Marco Angelini, Mauro Conti, and Selcuk Uluagac. 2023. Augmenting Security and Privacy in the Virtual Realm: An Analysis of Extended Reality Devices. *IEEE Security & Privacy*.

[16] Janet X Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. 2022. Trauma-informed computing: Towards safer technology experiences for all. In *Proceedings of the 2022 CHI conference on human factors in computing systems*. 1–20.

[17] Erika Chin, Adrienne Porter Felt, Vyas Sekar, and David Wagner. 2012. Measuring user confidence in smartphone security and privacy. In *Proceedings of the eighth symposium on usable privacy and security*. 1–16.

[18] Jessica Colnago, Lorrie Faith Cranor, Alessandro Acquisti, and Kate Hazel Stanton. 2022. Is it a concern or a preference? An investigation into the ability of privacy scales to capture and distinguish granular privacy constructs. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 331–346.

[19] Intersoft Consulting. 2018. General Data Protection Regulation (GDPR). https://gdpr-info.eu/

[20] Lorrie Faith Cranor. 2022. Mobile-app privacy nutrition labels missing key ingredients for success. *Commun. ACM* 65, 11, 26–28.

[21] Brendan David-John, Diane Hosfelt, Kevin Butler, and Eakta Jain. 2021. Let's SOUP up XR: Collected thoughts from an IEEE VR workshop on privacy in mixed reality. In *VR4Sec: Security for VR and VR for Security, SOUPS 2021 Workshop*.

[22] Elmira Deldari, Diana Freed, Julio Poveda, and Yaxing Yao. 2023. An investigation of teenager experiences in social virtual reality from teenagers', parents', and bystanders' perspectives. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. 1–17.

[23] Ellysse Dick. 2021. *Balancing user privacy and innovation in augmented and virtual reality*. Technical Report. Information Technology and Innovation Foundation.

[24] Nora A Draper and Joseph Turow. 2019. The corporate cultivation of digital resignation. *New media & society* 21, 8, 1824–1839.

[25] The Economist. 2020. Headset technology is cheaper and better than ever. https://www.economist.com/technology-quarterly/2020/10/01/headset-technology-is-cheaper-and-better-than-ever

[26] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the Experts: What Should Be on an IoT Privacy and Security Label?. In *2020 IEEE Symposium on Security and Privacy (SP)*. 447–464. https://doi.org/10.1109/SP40000.2020.00043

[27] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. 2023. Are Consumers Willing to Pay for Security and Privacy of IoT Devices?

[28] Interaction Design Foundation. 2024. Extended Reality (XR). https://www.interaction-design.org/literature/topics/extended-reality-xr

[29] Patricia I Fusch Ph D and Lawrence R Ness. 2015. Are we there yet? Data saturation in qualitative research.

[30] Andrea Gallardo, Chris Choy, Jaideep Juneja, Efe Bozkir, Camille Cobb, Lujo Bauer, and Lorrie Cranor. 2023. Speculative privacy concerns about AR glasses data collection. *Proceedings on Privacy Enhancing Technologies* 4, 416–435.

[31] Gonzalo Munilla Garrido, Vivek Nair, and Dawn Song. 2023. SoK: Data Privacy in Virtual Reality. *arXiv preprint arXiv:2301.05940*.

[32] Christine Geeng, Mike Harris, Elissa Redmiles, and Franziska Roesner. 2022. " Like Lesbians Walking the Perimeter": Experiences of {US}.{LGBTQ+} Folks With Online Security, Safety, and Privacy Advice. In *31st USENIX Security Symposium (USENIX Security 22)*. 305–322.

[33] Github. 2023. VRCX. https://github.com/vrcx-team/VRCX

[34] Lea Gröber, Rafael Mrowczynski, Nimisha Vijay, Daphne A Muller, Adrian Dabrowski, and Katharina Krombholz. 2023. To Cloud or not to Cloud: A Qualitative Study on {Self-Hosters}'Motivation, Operation, and Security Mindset. In *32nd USENIX Security Symposium (USENIX Security 23)*. 2491–2508.

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

[36] Camille Harris, Amber Gayle Johnson, Sadie Palmer, Diyi Yang, and Amy Bruckman. 2023. " Honestly, I Think TikTok has a Vendetta Against Black Creators": Understanding Black Content Creator Experiences on TikTok. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW2, 1–31.

[37] Sandra Höltervennhoff, Philip Klostermeyer, Noah Wöhler, Yasemin Acar, and Sascha Fahl. 2023. {"I} wouldn't want my unsafe code to run my {pacemaker"}: An Interview Study on the Use, Comprehension, and Perceived Risks of Unsafe Rust. In *32nd USENIX Security Symposium (USENIX Security 23)*. 2509–2525.

[38] Ismat Jarin, Yu Duan, Rahmadi Trimananda, Hao Cui, Salma Elmalaki, and Athina Markopoulou. 2023. BehaVR: User Identification Based on VR Sensor Data. (2023). arXiv:arXiv preprint arXiv:2308.07304

[39] Frederike Jung, Jonah-Noël Kaiser, Kai Von Holdt, Wilko Heuten, and Jochen Meyer. 2023. The Art of Privacy–A Theatrical Privacy Installation in Virtual Reality. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*. ACM, Hamburg, Germany, 1–5.

[40] Paul E Ketelaar and Mark Van Balen. 2018. The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. In *Computers in Human Behavior*, Vol. 78. Elsevier, 174–182.

[41] Yeji Kim. 2022. Virtual Reality Data and Its Privacy Regulatory Challenges: A Call to Move Beyond Text-Based Informed Consent. https://static1.squarespace.com/static/640d6616cc8bbb354ff6ba65/t/6445d2fbe62dac013aa91787/1682297596386/Kim-35-postEIC.pdf

[42] Lydia Kraus, Tobias Fiebig, Viktor Miruchna, Sebastian Möller, and Asaf Shabtai. 2015. Analyzing end-users' knowledge and feelings surrounding smartphone security and privacy. In *S&P. IEEE*. IEEE.

[43] Lydia Kraus, Ina Wechsung, and Sebastian Möller. 2016. Exploring psychological need fulfillment for security and privacy actions on smartphones. In *Proceedings of EuroUSEC*.

[44] Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. 2011. We're in it together: interpersonal management of disclosure in social network services. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 3217–3226.

[45] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. In *Proceedings of the ACM on human-computer interaction*, Vol. 2. ACM New York, NY, USA, 1–31.

[46] Kiron Lebeck. 2019. *Security and Privacy for Emerging Augmented Reality Technologies*. Ph. D. Dissertation.

[47] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. 2018. Towards security and privacy for multi-user augmented reality: Foundations

with end users. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 392–408.

[48] Jingjie Li, Sunpreet Singh Arora, Kassem Fawaz, Younghyun Kim, Can Liu, Sebastian Meiser, Mohsen Minaei, Maliheh Shirvanian, and Kim Wagner. 2023. " I Want the Payment Process to be Cool": Understanding How Interaction Factors into Security and Privacy Perception of Authentication in Virtual Reality. (2023). arXiv:arXiv preprint arXiv:2303.11575

[49] Jonathan Liebers, Mark Abdelaziz, Lukas Mecke, Alia Saad, Jonas Auda, Uwe Gruenefeld, Florian Alt, and Stefan Schneegass. 2021. Understanding user identification in virtual reality through behavioral biometrics and the effect of body normalization. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–11.

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

[51] Jialiu Lin, Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. 2012. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM conference on ubiquitous computing*. 501–510.

[52] Jinghuai Lin and Marc Erich Latoschik. 2022. Digital body, identity and privacy in social virtual reality: A systematic review. *Frontiers in Virtual Reality* 3, 974652.

[53] Xiao Ma, Jeff Hancock, and Mor Naaman. 2016. Anonymity, intimacy and self-disclosure in social media. In *Proceedings of the 2016 CHI conference on human factors in computing systems*. 3857–3869.

[54] Mohd Aliff Abdul Majid, Mohhidin Othman, Siti Fatimah Mohamad, Sarina Abdul Halim Lim, Aziz Yusof, et al. 2017. Piloting for interviews in qualitative research: Operationalization and lessons learnt. In *International Journal of Academic Research in Business and Social Sciences*, Vol. 7. 1073–1080.

[55] Nathan Malkin, Serge Egelman, and David Wagner. 2019. Privacy controls for always-listening devices. In *Proceedings of the New Security Paradigms Workshop*. 78–91.

[56] Divine Maloney, Guo Freeman, and Andrew Robb. 2020. A virtual space for all: Exploring children's experience in social virtual reality. In *Proceedings of the Annual Symposium on Computer-Human Interaction in Play*. 472–483.

[57] Divine Maloney, Samaneh Zamanifard, and Guo Freeman. 2020. Anonymity vs. familiarity: Self-disclosure and privacy in social virtual reality. In *Proceedings of the 26th ACM Symposium on Virtual Reality Software and Technology*. 1–9.

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

[59] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on human-computer interaction* 3, CSCW, 1–23.

[60] Meta. 2023. Detecting violations. https://transparency.fb.com/enforcement/detecting-violations/

[61] Meta. 2023. Hate Speech. https://transparency.fb.com/policies/community-standards/hate-speech

[62] Meta. 2023. Violent and Graphic Content. https://transparency.fb.com/policies/community-standards/violent-graphic-content/

[63] Meta. 2024. Supplemental Meta Platforms Technologies Privacy Policy. https://www.meta.com/legal/privacy-policy/

[64] Abraham Hani Mhaidli and Florian Schaub. 2021. Identifying manipulative advertising techniques in xr through scenario construction. In *Proceedings of the 2021 chi conference on human factors in computing systems*. 1–18.

[65] Mark Roman Miller, Fernanda Herrera, Hanseul Jun, James A Landay, and Jeremy N Bailenson. 2020. Personal identifiability of user tracking data during observation of 360-degree VR video. In *Scientific Reports*, Vol. 10. Nature Publishing Group UK London, 17404.

[66] Vivek Nair, Gonzalo Munilla Garrido, and Dawn Song. 2022. Going incognito in the metaverse. In *arXiv preprint arXiv:2208.05604*.

[67] Vivek Nair, Wenbo Guo, Justus Mattern, Rui Wang, James F O'Brien, Louis Rosenberg, and Dawn Song. 2023. Unique identification of 50,000+ virtual reality users from head & hand motion data. (2023). arXiv:arXiv preprint arXiv:2302.08927

[68] Vivek Nair, Christian Rack, Wenbo Guo, Rui Wang, Shuixian Li, Brandon Huang, Atticus Cull, James F O'Brien, Louis Rosenberg, and Dawn Song. 2023. Inferring Private Personal Attributes of Virtual Reality Users from Head and Hand Motion Data. (2023). arXiv:arXiv preprint arXiv:2305.19198

[69] 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.

[70] Fiachra O'Brolcháin, Tim Jacquemard, David Monaghan, Noel O'Connor, Peter Novitzky, and Bert Gordijn. 2016. The convergence of virtual reality and social networks: threats to privacy and autonomy. In *Science and engineering ethics*, Vol. 22. Springer, 1–29.

[71] Ken Pfeuffer, Matthias J Geiger, Sarah Prange, Lukas Mecke, Daniel Buschek, and Florian Alt. 2019. Behavioural biometrics in VR: Identifying people from body motion and relations in virtual reality. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.

[72] M Poikela and Felix Kaiser. 2016. 'it is a topic that confuses me'–privacy perceptions in usage of location-based applications. In *European Workshop on Usable Security (EuroUSEC)*.

[73] Alec Radford, Jong Wook Kim, Tao Xu, Greg Brockman, Christine McLeavey, and Ilya Sutskever. 2022. Robust speech recognition via large-scale weak supervision. https://cdn.openai.com/papers/whisper.pdf

[74] Ashwini Rao and Juergen Pfeffer. 2020. Types of privacy expectations. *Frontiers in big Data* 3, 7.

[75] Ashwini Rao, Florian Schaub, Norman Sadeh, Alessandro Acquisti, and Ruogu Kang. 2016. Expecting the unexpected: Understanding mismatched privacy expectations online. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. 77–96.

[76] RecRoom. 2021. Ensuring "Be Excellent to Each Other". https://blog.recroom.com/posts/2021/11/19/ensuring-be-excellent-to-each-other

[77] Lauren Reichart Smith, Kenny D Smith, and Matthew Blazka. 2017. Follow me, what's the harm: Considerations of catfishing and utilizing fake online personas on social media. *J. Legal Aspects Sport* 27, 32.

[78] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, Serge Egelman, et al. 2018. "Won't somebody think of the children?" examining COPPA compliance at scale. In *The 18th Privacy Enhancing Technologies Symposium (PETS 2018)*.

[79] Jacqueline M Roehl and Darci J Harland. 2022. Imposter participants: Overcoming methodological challenges related to balancing participant privacy with data quality when using online recruitment and data collection. In *The qualitative report*, Vol. 27. The Qualitative Report, 2469–2485.

[80] Louis B Rosenberg. 2022. Regulating the Metaverse, a Blueprint for the Future. In *International Conference on Extended Reality*. Springer, 263–272.

[81] Benjamin Saunders, Julius Sim, Tom Kingstone, Shula Baker, Jackie Waterfield, Bernadette Bartlam, Heather Burroughs, and Clare Jinks. 2018. Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality & quantity* 52, 1893–1907.

[82] Robert Soden, Austin Toombs, and Michaelanne Thomas. 2024. Evaluating interpretive research in HCI. *Interactions* 31, 1, 38–42.

[83] Daniel J Solove. 2007. I've got nothing to hide and other misunderstandings of privacy. *San Diego L. Rev.* 44, 745.

[84] Jessica Staddon, David Huffaker, Larkin Brown, and Aaron Sedley. 2012. Are privacy concerns a turn-off? Engagement and privacy in social networks. In *Proceedings of the eighth symposium on usable privacy and security*. 1–13.

[85] Nili Steinfeld. 2016. "I agree to the terms and conditions":(How) do users read privacy policies online? An eye-tracking experiment. *Computers in human behavior* 55, 992–1000.

[86] Anselm Strauss and Juliet Corbin. 1990. *Basics of qualitative research*. Sage publications.

[87] Zihao Su, Kunlin Cai, Reuben Beeler, Lukas Dresel, Allan Garcia, Ilya Grishchenko, Yuan Tian, Christopher Kruegel, and Giovanni Vigna. 2024. Remote Keylogging Attacks in Multi-user VR Applications. In *33rd USENIX Security Symposium (USENIX Security 24)*. USENIX Association, Philadelphia, PA, 2743–2760. https://www.usenix.org/conference/usenixsecurity24/presentation/su-zihao

[88] Philipp Sykownik, Divine Maloney, Guo Freeman, and Maic Masuch. 2022. Something personal from the metaverse: goals, topics, and contextual factors of self-disclosure in commercial social VR. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–17.

[89] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. 2019. " I don't own the data": End User Perceptions of Smart Home Device Data Practices and Risks. In *Fifteenth symposium on usable privacy and security (SOUPS 2019)*. 435–450.

[90] Jennifer EF Teitcher, Walter O Bockting, José A Bauermeister, Chris J Hoefer, Michael H Miner, and Robert L Klitzman. 2015. Detecting, preventing, and responding to "fraudsters" in internet research: ethics and tradeoffs. In *Journal of Law, Medicine & Ethics*, Vol. 43. Cambridge University Press, 116–133.

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

[92] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un) informed consent: Studying GDPR consent notices in the field. In *Proceedings of the 2019 acm sigsac conference on computer and communications security*. 973–990.

[93] Aliza Vigderman. 2024. Virtual Reality Awareness and Adoption Report. https://www.security.org/digital-security/virtual-reality-annual-report/

[94] Martin Vondráček, Ibrahim Baggili, Peter Casey, and Mehdi Mekni. 2023. Rise of the metaverse's immersive virtual reality malware and the man-in-the-room attack & defenses. *Computers & Security* 127, 102923.

[95] VRChat. 2024. Developer Update – 22 November 2023. https://ask.vrchat.com/t/developer-update-22-november-2023/20878/65

[96] VRChat. 2024. Privacy Policy. https://hello.vrchat.com/privacy
[97] Jason Watson, Andrew Besmer, and Heather Richter Lipford. 2012. + Your circles: sharing behavior on Google+. In *Proceedings of the eighth symposium on usable privacy and security*. 1–9.
[98] Dominik Wermke, Noah Wöhler, Jan H Klemmer, Marcel Fourné, Yasemin Acar, and Sascha Fahl. 2022. Committed to trust: A qualitative study on security & trust in open source software projects. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1880–1896.
[99] Rebecca Wong. 2021. Guidelines to Incorporate Trauma-Informed Care Strategies in Qualitative Research. Urban Institute.
[100] Yi Wu, Cong Shi, Tianfang Zhang, Payton Walker, Jian Liu, Nitesh Saxena, and Yingying Chen. 2023. Privacy Leakage via Unrestricted Motion-Position Sensors in the Age of Virtual Reality: A Study of Snooping Typed Input on Virtual Keyboards. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 3382–3398.
[101] Zhuolin Yang, Zain Sarwar, Iris Hwang, Ronik Bhaskar, Ben Y. Zhao, and Haitao Zheng. 2024. Can Virtual Reality Protect Users from Keystroke Inference Attacks?. In *33rd USENIX Security Symposium (USENIX Security 24)*. USENIX Association, Philadelphia, PA, 2725–2742. https://www.usenix.org/conference/usenixsecurity24/presentation/yang-zhuolin
[102] Powen Yao, Vangelis Lympouridis, and Michael Zyda. 2021. Virtual equipment system: face mask and voodoo doll for user privacy and self-expression options in virtual reality. In *2021 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*. IEEE, 747–748.
[103] YouTube. 2023. How does YouTube address misinformation? https://www.youtube.com/howyoutubeworks/our-commitments/fighting-misinformation/
[104] Mohammad Maifi Hasan Khan Yusuf Albayram and Michael Fagan. 2017. A Study on Designing Video Tutorials for Promoting Security Features: A Case Study in the Context of Two-Factor Authentication (2FA). In *International Journal of Human–Computer Interaction*, Vol. 33. Taylor & Francis, 927–942.
[105] Koosha Zarei, Reza Farahbakhsh, and Noel Crespi. 2019. Deep dive on politician impersonating accounts in social media. In *2019 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 1–6.
[106] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security and privacy concerns with smart homes. In *thirteenth symposium on usable privacy and security (SOUPS 2017)*. 65–80.
[107] Kexin Zhang, Elmira Deldari, Yaxing Yao, and Yuhang Zhao. 2023. A Diary Study in Social Virtual Reality: Impact of Avatars with Disability Signifiers on the Social Experiences of People with Disabilities. ACM.
[108] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User perceptions of smart home IoT privacy. In *Proceedings of the ACM on human-computer interaction*, Vol. 2. ACM New York, NY, USA, 1–20.

7 Appendix

7.1 Screening Survey

Consent Form

What are some general things you should know about research studies?
You are invited to take part in a research study. Your participation in this study is voluntary. You have the right to be a part of this study, to choose not to participate, and to stop participating at any time without penalty. This research study aims to understand users' perspectives on VR. We will do this through semi-structured user interviews.

Am I eligible to be a participant in this study?
To be a participant in this study, you must be at least 18 years of age, reside in the US, and currently use at least one VR application.

What will happen if you take part in the study?
If you agree to participate in this study, you will be asked to do all of the following:

- You will be asked to fill out a screening survey (the one you are currently filling out). The survey should take you around 5 minutes to complete.
- If you have been selected for an interview after the screening, you will be interviewed (remotely through video conferencing via Zoom), where you will be asked to share your experience in VR. We expect the interview to take around 60 minutes to complete. The interview will be audio recorded, transcribed, and the audio will then be deleted. You will be asked to turn on your video for a few seconds before the audio recording begins, making your face and VR headset visible for verification purposes. The video data will not be used for further analysis.
- Once the interview is complete, you will be asked to fill out another Qualtrics survey. This should take around 5 minutes.

Recording and Images
If you want to participate in this research, you must agree to turn on your video for verification (only for a few seconds, and it will not be recorded) and be audio recorded (the audio data would be used for research). You cannot participate in this research if you disagree with being audio recorded.

Risks and Benefits
There are minimal risks associated with participation in this research. The risks to you due to this research include distress due to recounting potentially upsetting past experiences while using VR. There are no direct benefits to your participation in the research. The indirect benefit is the improvement of VR user experience that arises from the insights derived from this research.

Right to withdraw your participation
You can stop participating in the study by withdrawing from being interviewed at any time for any reason. To do so, inform the researcher, [CONTACT INFORMATION]. You can also contact the faculty advisor for this research, [CONTACT INFORMATION]. If you choose to withdraw your consent and to stop participating in this research, you can expect that the researcher(s) will redact your data from their data set, securely destroy your data, and prevent future uses of your data for research purposes wherever possible. However, if you withdraw from the study, you will also forfeit your right to any compensation for participating in the study.

Confidentiality, Personal privacy, and Data management
Data that will be shared with others about you will be de-identified. De-identified data is information that at one time can directly identify you, but we will record this data so that your identity will be separated from the data. We do not have a master list with your code and real name that connects your information to the research data. When the research concludes, there will be no way your real identity will be linked to the data we publish.

Compensation
If you are selected for the interview, you will receive an Amazon e-gift card worth 20 USD for participating in the interview. If you withdraw from the interview process or choose to end your interview prematurely, you will not receive any compensation.

What if you have questions about your rights as a research participant?
If you feel you have not been treated according to the descriptions in this form, or your rights as a participant in research have been violated during the course of this project, you may contact the [University] IRB (Institutional Review Board) office. An IRB office helps participants if they have any issues regarding research activities.

Qualifying Questions

- I am at least 18 years old
- I am a resident of the United States
- I currently use at least one Virtual Reality application
- I agree to turn on my video for a few seconds before the audio recording begins, making my face and VR headset visible. I understand that this will be used for verification purposes.
- I affirm that I have read and understood the above information, and all the information I provide is true and correct to the best of my knowledge. All of the questions that I had about this research have been answered. I have chosen to participate in this study with the understanding that I may stop participating at any time; if I withdraw from the study I will forfeit my right to compensation.I am aware that I may revoke my consent at any time.

VR Usage

- How long have you used VR?
  - < 1 month
  - >= 1 month but < 1 year
  - >= 1 year but < 2 years
  - >= 2 years but < 3 years
  - >= 3 years but < 4 years
  - >= 4 years
- How many hours do you spend in VR on average per week?
  - 0 hours (I currently do not use VR)
  - 1 to 4 hours
  - 5 to 9 hours
  - 10 to 14 hours
  - 15 to 19 hours
  - 20 hours or more
- When was the last time you used VR? (if 0 hours was selected for previous question)
- Which VR Headset(s) do you use?
  - Meta Quest
  - HTC Vive
  - HP Reverb
  - Sony Playstation VR
  - Valve Index VR kit
  - Oculus Rift
  - Samsung Gear VR
  - Other
- What activities do you use VR for? Select all that apply.
  - Socializing
  - Playing games
  - Attending virtual events
  - Learning about something
  - Physical fitness related activities
  - Mental health related activities
  - Others (Please specify)
- Name the VR Apps you use most frequently (please mention as many apps as you can).

Demographics

- What is the highest level of education you have completed?
  - Less than high school
  - High school or equivalent
  - Some college
  - Trade, technical or vocational training
  - Associate's degree
  - Bachelor's degree
  - Master's degree
  - Doctoral degree
  - Professional degree (JD, MD, etc.)
  - Other (please specify)
  - Prefer not to answer
- Please indicate your age range.
  - 18-24
  - 25-34
  - 35-44
  - 45-54
  - 55-64
  - 65-74
  - 75-84
  - 85 and above
- Which of the following best describes your gender?
  - Man
  - Woman
  - Non-binary
  - Prefer to self-describe (please specify)
  - Prefer not to answer
- Which of the following best describes your sexual orientation?
  - Heterosexual (straight)
  - Homosexual (gay)
  - Bisexual
  - Prefer to self-describe (please specify)
  - Prefer not to answer
- Choose one or more of the races you consider yourself to be:
  - American Indian or Alaskan Native
  - Hispanic, Latinx, or Spanish origin
  - Caucasian
  - Asian
  - Black or African American
  - Middle Eastern or North African
  - Native Hawaiian or Pacific Islander
  - Other (please specify)
  - Prefer not to answer

7.2 Participant demographics

Table 3 contains the self-reported demographic details of all the participants in our study.

7.3 Interview Protocol

Hi there! Thank you for participating in our study! My name is [Insert Name] and this is [Insert Second Name]. Today, we will be having a chat about your use of virtual reality. Before we get started, I want to make sure you understand all the details of the study. When you filled out the sign-up form, you agreed to all the requirements in the consent form for this research study. Would you like to have a look at the consent form again, or do you want to have a copy of it?

In the consent form, you agreed to turn on your video for a few seconds so that we can verify your identity and ensure that you are a VR user. Can you please turn on your video and show us your VR headset?

Table 3: Participant demographics (self-reported).

ID	Age	Gender	Sexual Orientation	Race	S&P Education	Headset Used	Usage (years)	Usage (hrs/week)
P1	35-44	Man	Heterosexual	Prefer not to answer	Formal Training	Meta Quest	>= 4 years	5 to 9 hours
P2	18-24	Man	Heterosexual	Caucasian	None	Meta Quest	>= 2 years but < 3 years	5 to 9 hours
P3	55-64	Man	Heterosexual	Caucasian	Acquired Education	Meta Quest	>= 4 years	10 to 14 hours
P4	18-24	Man	Bisexual	Caucasian	Formal Training	Valve Index	>= 4 years	10 to 14 hours
P5	45-54	Man	Heterosexual	Caucasian	Trained against Phishing scams	Meta Quest	>= 4 years	10 to 14 hours
P6	25-34	Man	Heterosexual	Caucasian	Acquired Education	Meta Quest, Valve Index	>= 4 years	5 to 9 hours
P7	18-24	Man	Bisexual	Caucasian	None	Meta Quest	>= 4 years	1 to 4 hours
P8	18-24	Woman	Bisexual	Caucasian	None	HTC Vive, Valve Index	>= 2 years but <3 years	1 to 4 hours
P9	35-44	Man	Heterosexual	Hispanic, Latinx, or Spanish origin, Caucasian	Trained against Phishing scams	HTC Vive, Valve Index	>= 4 years	10 to 14 hours
P10	25-34	Woman	Pansexual	Caucasian	None	Valve Index	>= 3 years but <4 years	20 hours or more
P11	25-34	Woman	Bisexual	Caucasian	None	Meta Quest	>= 1 year but <2 years	5 to 9 hours
P12	25-34	Woman	Bisexual	Caucasian	Acquired Education	Valve Index	>= 1 year but <2 years	15 to 19 hours
P13	18-24	Man	Heterosexual	Black or African American	None	Valve Index VR kit	>= 3 years but <4 years	10 to 14 hours
P14	18-24	Non-binary	Homosexual	Caucasian	None	Meta Quest	>= 2 years but <3 years	15 to 19 hours
P15	25-34	Man	Heterosexual	Hispanic, Latinx, or Spanish origin	None	Meta Quest	>= 3 years but <4 years	5 to 9 hours
P16	35-44	Man	Heterosexual	Hispanic, Latinx, or Spanish origin	Formal Training	Meta Quest, Oculus Rift	>= 2 years but <3 years	1 to 4 hours
P17	35-44	Man	Heterosexual	Hispanic, Latinx, or Spanish origin, Caucasian	Trained against Phishing scams	Meta Quest	>= 2 years but <3 years	5 to 9 hours
P18	25-34	Woman	Bisexual	Hispanic, Latinx, or Spanish origin, Caucasian	Trained against Phishing scams	Meta Quest, Valve Index	>= 2 years but <3 years	5 to 9 hours
P19	25-34	Woman	Heterosexual	Caucasian	Acquired Education	Valve Index	>= 1 month but <1 year	1 to 4 hours
P20	35-44	Woman	Bisexual	Caucasian	Acquired Education	Meta Quest	>= 2 years but <3 years	5 to 9 hours

Thank you, you can turn off your video if you want to. In the consent form, you agreed to be audio recorded. Could you please confirm that you allow us to audio-record this interview?

Thank you. As you know, this discussion is being audio recorded. After the researchers transcribe the recording, the audio will be deleted. Your name, contact information, and other forms of personally identifying information will not be asked or recorded during this discussion, and will not be used while presenting any results of this study. At the end of our chat, I will share another survey, which will ask you to provide your name and address for our accounting office to process your compensation. We will not store this information along with our transcripts. Our discussion today would take around 1 hour to complete. At this point, do you have any questions?

I would like to begin with a few questions about your current use of VR.

- I see you've mentioned that you have been using VR for(duration). What made you decide to use VR?
- I see you've mentioned that you use VR for (activities). What motivated you to do [listed activity] in VR? How's your experience so far?
- Are there any aspects of the activities you do in VR that you consider private?
  - Yes
    - What aspects of your activities are private to you?
    - Why do you consider them private?
    - Do you believe any information related to these activities could be known by other parties?
      - Who are these parties, according to you?
      - Why do you think they collect this information?
      - How do you think this information is used?
  - No
    - Why not?
  - Never thought about it
    - When was the last time you chatted with other people? Probes specific to their VR activities.
- Have you come across any privacy related issues in VR?
- Before deciding to use a particular VR app, do you consider the privacy aspects associated with it?
  - What do you specifically look at?
  - What additional things would you like to look at?
- Here are a few major providers of VR platforms. How much have you heard about each of them?
- Let me share a few images with you (share screen and open pdf consisting of screenshots of one or more apps based on screening survey). These are screenshots of a few <type> VR apps, as shown on an existing app store for VR. As such, our questions are also about <type> VR apps as a whole category rather than specific <type> VR apps. I want to mention that the data collected depends on the app and not the headset / platform. Even though we are not showing you the app info from [platform-name], the underlying data practices would be very similar. Imagine that the app is collecting this data. What are your thoughts?
  - In the image, you can see what kind of specified information about you and your device these apps can access. Are any of these sensitive to you?
    - Who (apart from app developers) do you think might have access to this information?
    - Why do you think they collect this information?
    - How do you think this information is used?
  - Are you concerned by this?
    If yes Do you do anything about this? How would you want this information to be handled?
    If no Why not?
  - In any of the apps you use, would you willingly share some information with vr app developers? Why / why not

  - In any of the apps you use, would you willingly share some information with people on VR? Why / why not
  - Of the apps that you use, are any of them paid?
    * Do you think data collection in paid and non-paid apps are similar or different?
- Moving on to a broader look at data collection in VR, do the privacy concerns that you mentioned earlier, influence how you use VR?
  - Yes
    * How do they influence your usage?
  - No
    * Why not?
- What specific privacy controls would you want for VR applications?
- How have your privacy considerations evolved over time?
- Would you recommend VR to a friend/colleague/family? Why or why not?
- Any additional concerns to share or discuss?
- Have you received education in privacy and security, or use these concepts in your job?

That brings us to the end of this discussion. Thank you so much for your time and all the valuable insights you've provided! I'm really glad that you decided to take part in our study. To record your completion of the interview, can you please fill out the post-interview survey?

Once again, thank you for participating, and have a great rest of your day! And feel free to reach out to me, if you want to share anything else.

7.4 Screenshots Presented

Figure 2: VR platforms presented to participants

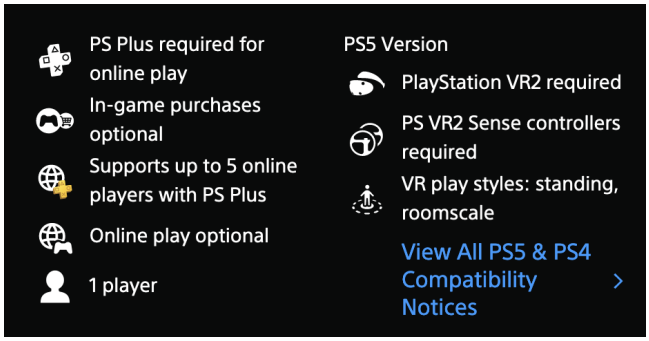
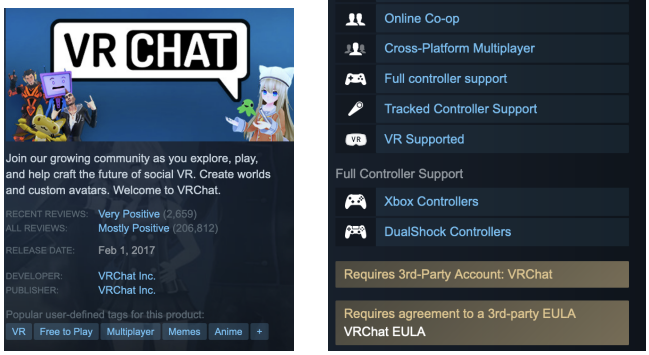
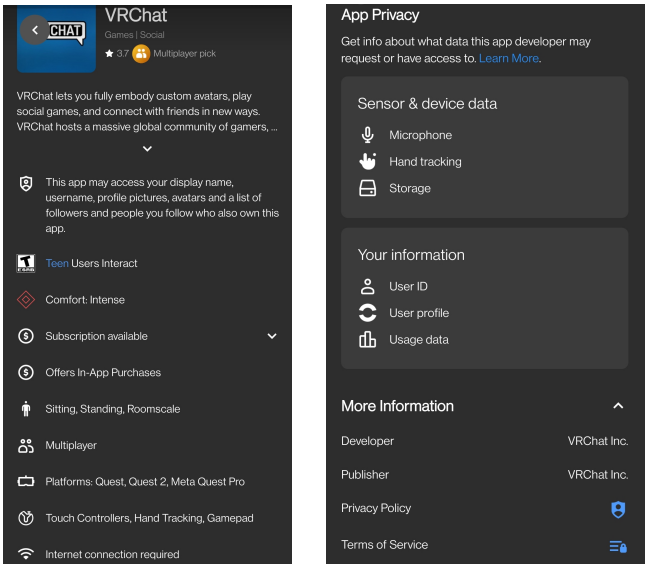


Figure 3: Screenshot showing details of Beat Saber from the PlayStation Store.



(a) basic app information (b) hardware and interaction features

Figure 4: Example screenshots showing details of VR Chat from the Steam Store.



(a) basic app information (b) types of data collected

Figure 5: Example screenshots showing details of VR Chat from the Meta Quest Store.