

More Modalities, More Problems: Examining User Understanding of The Meta Quest Permissions Framework

Sarah Radway
Harvard University
sradway@g.harvard.edu

Matthew Soto*
Carnegie Mellon University
mdsoto@andrew.cmu.edu

Suvi Lama*
Massachusetts Institute of Technology
suvilama@mit.edu

Carson Powers
Tufts University
cpower04@cs.tufts.edu

Daniel Votipka
Tufts University
dvotipka@cs.tufts.edu

Abstract

Compared with preceding consumer technologies, virtual reality (VR) requires extensive collection of sensitive biometric data. On the Meta Quest 2 (the most popular consumer headset), application access to sensitive data is mediated by a *permissions system* adapted from Android's model. In this work, we examine how VR's immersive nature necessitates new permissions considerations beyond preceding technology and current VR devices. We analyze the Meta Quest 2's permissions system, identifying where it diverges from Android's user-facing behavior surrounding biometric data. We then investigate the implications of both conventional Android and novel Quest permission flows through an in-person VR interview study with 23 participants. We observe that many participants lacked awareness of how VR collects data or the extent of passive tracking in VR. Based on these findings, we offer recommendations for VR permissions models and suggest directions for future work.

Keywords

virtual reality, permissions, VR/AR/XR, privacy

1 Introduction

Virtual reality (VR) devices collect and use extensive biometric data to provide a comfortable and immersive user experience. Misalignment between a user's actual body position and virtual representation reduces their sense of realism; for example, the absence of hands in a virtual experience disrupts bodily presence, as users are accustomed to seeing their hands in the field of view [29]. Therefore, VR devices seek to provide realistic representations of user behavior, in order to provide pleasant, immersive experiences.

Providing realistic representations in VR requires input from numerous sensors. For example, Meta's Quest Pro, a popular consumer VR headset, uses five inward-facing infrared cameras on the headset to track the user's face and eyes, five outward-facing cameras to track their surroundings, body, and hands, and three cameras on each controller to track their movement [100]. Meta Quest headsets and controllers also contain an Internal Measurement Unit

(IMU) with a series of sensors (e.g., gyroscopes, accelerometers) to supplement positional data provided by the cameras [55]. This represents a significant increase in data sources compared with preceding consumer technology; while an Android mobile phone can broadly track a device's movement using an accelerometer [17], a Meta Quest 2 can use its cameras to track up to 26 joints on just the user's hand [78].

To prevent delays or mismatches between real-world actions and virtual representations, biometric data must also be collected and processed frequently. Low frame rates or tracking errors desynchronize a user's display from their real-world movement, causing discomfort or nausea [98, 110]. Therefore, VR data is also sampled at more frequent intervals than preceding technology. Although smartphones generally contain an IMU, their capability is limited—Android devices cap their sensor sampling rate at 200 Hz [16], whereas Meta Quest IMUs have a max sampling rate of 1kHz [81]. This increases the volume of user data collected in VR.

This data is not only identifying—it also reflects how data features change over time in different contexts. While smartphones may use facial recognition [94] or collect fingerprint data [95] to authenticate individuals, these are static features; they are collected once, and remain stable. VR devices collect extensive dynamic data types, observing how biometric data features change over time under various circumstances. For example, eye tracking in VR not only captures images of a user's pupil, but also infers where they look and for how long. VR data's extensive collection frequency and depth presents significant, new privacy threats. Combined with machine learning, this tracking data can prove very invasive, revealing a user's identity, or other personal attributes, such as behavior, emotion, health, or physical appearance [84, 85, 101, 117].

Quest devices allow users to make decisions about biometric data collection and use through a *permissions system*. Permissions regulate application access to device hardware and software [14]. Some permissions are explicitly granted by users—typically those considered more sensitive (e.g., microphone access)—while others are granted automatically by the system—typically those viewed as less sensitive (e.g., Wi-Fi state) [44]. The Meta Quest 2 permissions system largely draws on established smartphone best practices [33, 43, 44, 62, 108, 114–116], adopting Android's framework directly.

However, data-collection modalities for VR and for traditional Android devices dramatically differ. Prior work has only examined the efficacy of Android's permissions model on smartphones [33, 43, 44, 62, 70, 108]; VR users are immersed in their environment and subject to data collection at an unprecedented scale to support device

*This work was performed primarily while the authors were affiliated with Tufts University.

This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license visit <https://creativecommons.org/licenses/by/4.0/> or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

Proceedings on Privacy Enhancing Technologies 2026(4), 438–454

© 2026 Copyright held by the owner/author(s).

<https://doi.org/10.56553/popets-2026-0129>



functionality. It is unclear whether permissions mechanisms will produce different behavior in this new, immersive modality. Moreover, VR introduces biometric data types not present on Android devices. For these novel data types, Meta employs new, non-standard permissions flows; below, we examine how Meta's biometric data permissions implementation departs from established Android best practices. It is therefore important to assess both how Meta strays from Android's permissions best practices and how user mental models of data collection shift in this immersive modality.

Contributions. In this work, we address three research questions:

(RQ1): How did Meta update the Android permission system to incorporate novel VR interaction modalities? We examine the implementation of the Quest permissions system, as compared with the Android Open Source Project (AOSP) permissions system. We identify differences surrounding how biometric data requests and usage are handled, both at the system and user levels. In particular, we highlight the implementation of a new *device-wide* permissions flow used for some biometric data. In this new permissions flow, users turn the permission on and off for all applications, not for each application individually.

(RQ2): What are users' understandings of the Quest 2 permissions implementation? We conducted in-depth interviews with 23 participants to evaluate the impact of the Meta Quest's data collection and permissions implementation on user privacy understanding. Previous work examining VR privacy beliefs uses non-immersive methods (e.g., online surveys), overlooking the immersive modality inherent in VR. Instead, our user study is informed by participant experiences with actual VR application use during our study. Participants used a series of applications with different biometric data collection permission requests on a Meta Quest 2 in a lab environment. We assessed participants' ability to recall permissions interactions and their understanding of these interactions. We found participants were broadly aware data collection was occurring, but did not understand how data was collected, and had misconceptions regarding the extent of collection. For the Meta Quest 2's new device-wide hand tracking permission flow, most participants *understood* the hand tracking permission was granted globally across apps. Some participants saw value in this approach, due to decreased friction when exiting and entering applications using hand tracking. Other participants indicated privacy concerns with this new permissions model, due to the potential for overreach associated with a global permissions toggle. We examine this tension between privacy and utility in Section 5.

(RQ3): What guides a user's mental model of data collection in immersive modalities? The permissions system is only a piece of the broader notice and choice framework; therefore, we also look beyond the permissions system, to investigate more broadly how the multi-modal nature of VR data impacts existing usability challenges. Our findings suggest participant perceptions of data collection in VR are largely driven by functionality of the application (similar to previous work in the Android space [83]). Participants were more likely to recall the data type's collection when application interfaces directly indicated use of a biometric data type as part of gameplay (e.g., hands were used to chop blocks). Additionally, some participants relied upon analogies from prior technology to build their mental models of Quest 2 data collection and use. While

useful for understanding data collection practices present in earlier technology, these mental models also carried assumptions from non-immersive contexts about advertising and third-party sharing.

Based upon our findings, we provide recommendations for permissions best practices in VR, as well as directions for future research to better understand the impact of immersive modalities on user permissions understanding.

2 Background

Virtual reality has grown in popularity over the past decade [99]. Initially, low frame rates and limited resolution constrained the usability of the technology [112]; however, as performance has improved, VR has seen widespread adoption in the consumer market. Today, 27% of U.S. adults own or have used a VR device [21].

In this paper, we focus on the most popular consumer VR device, the *Meta Quest 2* [104]. We selected this device because of its widespread adoption, which provides a valuable opportunity to examine contemporary consumer VR device behavior. Older (e.g., HTC Vive) and newer (e.g., Meta Quest Pro) headsets didn't similarly permeate the consumer market [11, 54]. The Quest 2 uses head tracking to update the field of view as the user moves, displaying a virtual environment for the user. It is operated with hand controllers, or users can optionally turn on hand tracking to replace controllers.

The Quest 2 operating system (OS) is built on top of the *Android Open Source Project* (AOSP), a base Android OS that consumer device producers adapt for their own product use cases [20]. This means the Quest 2 *permissions system* is derived from the AOSP. Permissions are mechanisms that moderate applications' access to device hardware and software, including access to user data [14]. Different AOSP permissions have different levels of potential harm to users. AOSP classifies the sensitivity of each permission with a *protection level*. Less sensitive permissions are called *normal permissions*; for example, the "ACCESS_WIFI_STATE" permission provides information about a device's network connection status. This permission is less sensitive—applications often require information about WiFi status to ensure functionality. In contrast, "ACCESS_BACKGROUND_LOCATION" allows an application to collect information about the device's location, even while the application is not open. This permission is more sensitive—users perceive location data as meriting additional privacy protections [103]. More sensitive permissions are called *dangerous permissions*. Lastly, some permissions data is only shared between applications signed with the same certificate. For example, Meta applications may want to communicate using internal system API calls, without other applications using the API. These are called *signature permissions*.

In Android systems, users are largely unaware when applications request normal or signature permissions, because they are granted automatically by the system without user interaction. Dangerous permissions are presented to users following the *Ask On First Use (AOFU)* permissions model; the user is prompted to grant the app permission to access sensitive data the first time the app requests that data type. If the user grants the permission, the app can make subsequent accesses to the sensitive data without further prompting the user. Additionally, data safety labels (short descriptions of privacy implications for data being requested) are included

on application download pages, to provide users with further details about each app's data collection practices. This provides an informed consent framework for sensitive data collection.

After the initial AOFU popup, users can modify app permissions in the device settings through two relevant pages [19]. One page lets users select an app from the list of installed apps and manage its permissions. The other page lets users select a permission and decide which apps are granted or denied access to it.

There is also a third page, "Special Permissions," which manages especially sensitive permissions that are given extra protections. For example, "Display over other apps" allows an application to display or draw over other apps without those apps' consent [40]. These permissions are rarely required by apps [15]. Users are required to enable the special permission for each application from this page.

2.1 Related Work

VR Privacy Threats. Recent work in the HCI domain has investigated potential privacy threats in VR—in particular, studies have examined the extent to which users can be identified using biometric data in VR [57, 84, 85], as well as the extent to which user behavior in immersive spaces can be identified by observers [47, 86]. These works are formatted as large scale experiments, rather than qualitative investigations, as these studies examine what can be learned from user data or behavior in VR, rather than interpreting *what users expect* from their VR interactions.

Most similar to our work, there exists a body of human factors work which aims to investigate user expectations in VR. These studies have investigated the extent to which VR users worry about physical harms (e.g., motion sickness), physical privacy concerns (e.g., camera data collection), or biometric privacy concerns (e.g., microphone data collection) [8, 52, 58, 96]. However, prior work primarily answers these questions via survey-based studies conducted online [8, 52, 58], and interview studies like S.B. et al. do not have participants use VR as part of the study [96]. To our knowledge, our study is the first to attempt to address these same questions of user privacy perceptions in more realistic settings, involving real-world device use. Our work provides a useful point of comparison by highlighting where theoretical and practical investigations converge or differ. For example, these studies report limited user awareness of XR sensor data collection; we show that this finding also holds in real-world, non-hypothetical settings.

Other works examined user perspectives on social privacy [36] and parent perspectives on child privacy in VR [32]. Mhaidli et al. also investigate user perceptions of VR advertisements, providing recommendations to align advertisers' practices in immersive environments with user expectations [82]. In contrast, our work examines how well users understand the permission systems designed to protect them from privacy threats.

VR Privacy Policies. Studies have also investigated statements made in VR application privacy policies [8, 50, 105, 118] and studies in the domain of systems research have verified the validity of these policy analyses through traffic analysis exercises [50, 105, 105]. These works have found that, much like in preceding technologies, VR app privacy policies are vague and often inaccurate.

AR Privacy Threats. There is also a substantial body of HCI work pertaining to general security and privacy concerns in *augmented*

reality (AR). This work enumerated novel concerns introduced by AR, such as more extensive input data collection, or intentional manipulation of display output to mislead the user [34, 67, 73, 93]. Abraham et al. propose a novel scheme for permissions in augmented reality [7]. Harborth et al. investigate the practices of AR smartphone applications, demonstrating the need for greater permissions-based control [53]. However, these works are largely focused on smartphone-based AR applications, like Snapchat or Pokemon Go. We extend this investigation to a new modality, namely, permissions within a popular consumer VR device. Additionally, O'Hagan investigates bystander (rather than user) privacy in AR [89].

Android Permissions System. Prior work has investigated the current Android permissions system, focusing on user comprehension [24, 26, 33, 44, 109], application use [113] and misuse [31, 43, 68, 102, 114], and security issues [9, 22, 31, 83, 106, 111]. Most relevant to our work are those focused on user comprehension. These studies aimed to address two features of permissions: whether users are well-informed enough to make informed decisions [33, 44, 90, 114], and whether mechanisms sufficiently provide users with the opportunities to make informed decisions [26, 33, 44, 70, 90, 114]. This body of work examining the Android permissions system was foundational in shaping the permissions system used by the Meta Quest. As we discuss in Section 3, the Meta Quest adapts this system to address the updated requirements of immersive modalities. Revisiting questions raised in prior research is essential for evaluating the effectiveness of these adaptations. *To our knowledge, there no prior work examining consumer VR device permissions systems.*

Privacy Mental Models and Privacy Frameworks. Privacy mental models refer to the cognitive mechanisms by which users conceptualize privacy, often using simplifying heuristics or metaphors. One widely discussed privacy mental model centers on contextual integrity, a theoretical framework that characterizes how individuals reason about privacy in everyday settings [87]—information flows are considered permissible when they align with prevailing social norms regarding appropriate data practices; conversely, departures from these norms are interpreted as violations of privacy.

Another influential privacy framework is the notice-and-choice framework. Within this regulatory paradigm, the responsibility for evaluating data collection and use practices is placed primarily on the individual user [71]. The framework presumes that users conceptualize privacy as a transactional exchange: acceptance of a notice signifies a voluntary trade of privacy for some perceived benefit, whereas refusal indicates an intention to retain privacy. In practice, users are routinely confronted with interface mechanisms (e.g., cookie banners) that compress complex privacy considerations into a momentary decision, reinforcing the notion that consent is a discrete transaction rather than a sustained, relational process. Our study examines the applicability of these mental models in VR, and the extent to which multi-modal data worsens preexisting challenges surrounding these mental models.

Previous work has examined the design and implementation of privacy notices, and of notice and choice frameworks more broadly. Some works examine user understanding of various implementations of privacy notices, examining existing practices for privacy policies [35, 97], providing technical best practices [35, 45, 97] or providing [45, 61, 71] proposals to improve the notice and choice ecosystem. Others examine user understanding of specific notice

and choice implementations; for example, examining GDPR privacy notices, and the downstream impact of presentation mechanisms on user comprehension and decision making [27, 48, 63, 65, 88, 107]. However, these investigations center on traditional, non-immersive modalities, such as smartphones or computer web browsers; no previous work considers how VR’s multi-modal data may worsen preexisting challenges with notice and choice frameworks.

3 RQ1 — Quest 2 Updates To The Permissions System

Because the Quest 2 is based on the Android OS, its core system code is largely derived from Android. We provide some context on the Android OS in Section 2. Here, we focus on how the Quest 2’s permissions implementation differs from that of the Android OS. To do so, we conduct a systematic review of changes to the Quest 2’s permissions system at both the system and user levels.

3.1 Systematic Review Methodology

To evaluate differences between Android and Quest 2 permission systems, two researchers collaboratively reviewed Quest 2 and Android UI elements, file system artifacts, and accessible operating system code using an inductive analysis approach to identify themes in what data is collected and how it is handled. One researcher has over a decade of industry and academic experience reverse engineering Android apps and the Android OS, including multiple publications in this area. The other has several years of academic and professional experience in Android reverse engineering.

Using Android Debug Bridge (ADB), we searched Quest system files for permission-related artifacts (e.g., manifests, permission validation logic, and UI components) using keywords such as “permission” and “manifest”. We focused primarily on operating system manifest files, which define supported permissions (i.e., their `protectionLevel` and `permissionGroup`) [13, 18, 46].

In Android-like systems, permissions must be defined in a manifest file using a `<permission>` entry [18]. We manually reviewed Quest 2 manifest files defining system permissions and compared them against the Android Open Source Project (AOSP) system manifest. [13, 46]. This analysis identified two primary Quest permission manifests: one closely aligned with AOSP and one Quest-specific manifest, containing additional permissions relevant to VR interaction. We then reviewed associated permission-handling code to understand how biometric permissions are implemented and exposed to applications.

To analyze user-facing permission behavior, we compared Android and Quest 2 permission interfaces, including Settings privacy pages and runtime permission dialogs. We also examined relevant files associated with these UI components (e.g., `SettingsPanelApp.apk`), grepping for text displayed in the Settings UI (e.g., “Headset Tracking”), and recursively following file references.

Following best practices [72], we do not calculate inter-rater agreement for this analysis because both researchers collaboratively performed the review and the results are not subjective. For example, the identified differences in system-level data availability are derived directly from differences in the manifest files and are

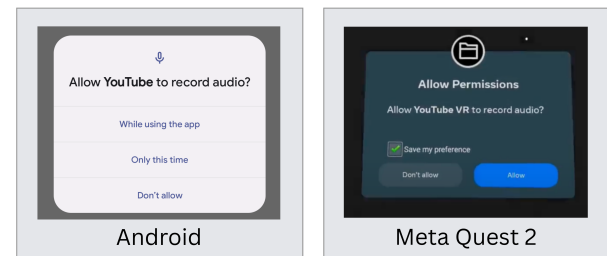


Figure 1: The microphone permissions flow on Android (left) and Meta Quest (right) operating systems.

not open to interpretation. If there were differences in interpretation, the researchers consulted documentation and discussed until mutual understanding as reached.

3.2 How does the Quest 2 align and diverge from AOSP regarding sensitive biometric data?

Third-party access to biometric data on Android is primarily mediated through the permissions system. Raw biometric data is generally protected by “dangerous” permissions, and biometric functions are exposed only through higher-level APIs. For example, fingerprint authentication APIs reveal only authentication outcomes rather than the underlying fingerprint data itself.

Quest developers operate under a similar but distinct model. Applications typically do not access raw sensor streams directly. Instead, they receive higher-level outputs such as joint-specific position coordinates for hand tracking. Although these abstractions limit direct exposure to biometric data, they can still reveal sensitive information about a user’s body, behavior, or attention. In this section, we examine how Quest’s permission system addresses this issue of sensitive, but abstracted, biometric data.

3.2.1 What stays the same? As discussed in Sections 2 and 3.1, the Quest 2 operating system is based on Android, and therefore retains much of Android’s existing permission model. Most permissions present in AOSP source code are also implemented on the Quest 2 with similar enforcement mechanisms. For example, “`android.permission.RECORD_AUDIO`” grants apps access to the microphone. In both Android and the Quest 2, this permission uses the “dangerous” protection level. As a result, apps requesting microphone access trigger an AOFU permission prompt that must be accepted before access is granted (see Figure 1).

3.2.2 What changes in the Quest 2? The functionality of the Quest 2 necessitates new forms of biometric data collection, including head, hand, and body tracking. These data types require invasive mechanisms, such as camera footage and frequent Internal Measurement Unit (IMU) sampling. Prior work demonstrates that they can support sensitive inferences; for example, recent studies show users can be uniquely identified through VR head and hand tracking data [69, 85]. As such, these data types would traditionally merit increased protection.

In Android, sensitive permissions are typically implemented using the “dangerous” protection level; permissions such as `RECORD_`

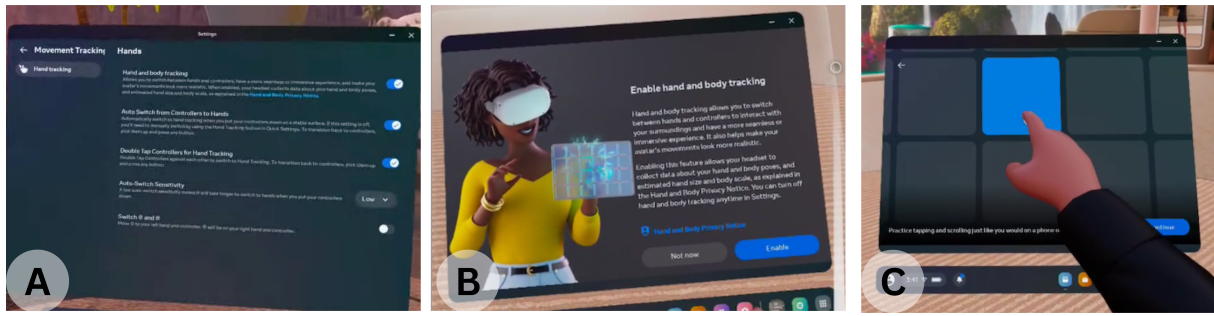


Figure 2: The novel hand tracking permissions flow on the Meta Quest 2, which is required to use applications with hand tracking. Box A shows the settings page where users must navigate to in order to turn on hand tracking. Box B shows the tutorial for hand tracking and privacy notice. Box C shows the tutorial for how to use hand tracking.

AUDIO, BODY_SENSORS, and ACTIVITY_RECOGNITION all follow this model. However, Quest 2 biometric permissions diverge from these conventions, using mechanisms that do not consistently align with Android’s traditional sensitive-permission model. We examine these implementations in greater depth below, focusing on how they differ from standard AOSP practices in both data sensitivity and user-facing behavior.

Headset Tracking. Headset tracking provides information about a user’s head orientation and position using IMU sensors (i.e., accelerometers, gyroscopes) [66]. Tracking may support either three degrees of freedom (3DoF), which captures rotational movement only, or 6DoF, which also captures positional movement [77].

The Quest 2 distinguishes between foreground and background access to head-tracking data. Foreground tracking does not require a system-level permission; instead, users can globally enable or disable 6DoF tracking through the “Headset Tracking” system setting, which is enabled by default. In contrast, background head tracking (which extends data access to when apps are not actively open) is protected by the `com.oculus.permission.ACCESS_BACKGROUND_HEAD_TRACKING` permission, which uses the signature|system protection level, limiting access to Meta-affiliated applications.

Hand Tracking. Hand tracking enables controller-free interaction by estimating the position of a user’s hands from outward-facing camera footage. The system fits a generic hand model to image data and estimates key points (i.e., fingers, knuckles) in real time [74, 76].

Third-party access to hand tracking data is governed by the `com.oculus.permission.HAND_TRACKING` permission, which is assigned the “normal” protection level. However, unlike traditional Android normal permissions, hand tracking can still be globally enabled/disabled via the “Hand and Body Tracking” setting, which presents users with a pop-up (Figure 2). This is somewhat similar to a “Special Permission” in traditional Android systems: a subset of permissions are controlled via a special Settings page. However, unlike traditional Android systems, app-by-app control over data access is not provided in the Quest 2 settings page—the setting applies across the whole app.

Body Tracking. Body tracking uses camera footage and IMU data from the headset and controllers to estimate a user’s body

pose [41, 74, 76]. `com.oculus.permission.BODY_TRACKING` is similarly assigned “normal” protection level. Interestingly, this permission on the Quest 2 was initially implemented as a dangerous permission; within the past year and a half, Meta downgraded the body tracking permission to a normal protection level. It is interesting that they choose to change this protection level—especially given the extent of recent research demonstrating that this data can be used to violate user privacy, as described in Section 2.

Body tracking is included in the global “Hand and Body Tracking” setting toggle, and users turn on this global permission for hand and body tracking together (See Figure 2). The Quest 2 grants this permission at run-time, without mandating an AOFU pop-up. When running the Meta SDK’s Native OpenXR body tracking sample, we see that body tracking began with no pop-up [79]; this is further confirmed by Meta documentation, which states that in order to create a body tracker, “your app must request the `com.oculus.permission.BODY_TRACKING` permission in the manifest, but a user is not requested to or required to grant this permission” [80].

Head, hand, and body tracking implementations diverge from standard Android permission conventions, and introducing novel interaction pathways that may differ from user expectations. Next, we discuss how these design choices may affect user understanding and subvert established permission expectations.

3.3 What usability implications might these divergences have?

These system-level design choices introduce several potential user-facing challenges. We identify three primary points of friction in the Quest 2 permission implementation.

3.3.1 The Quest 2 does not clearly communicate what data is collected when a permission is enabled. For the examined permissions, we observe limited transparency into what data is being collected, either by the operating system or by third party applications. At the time of our study, the onboarding flow for hand and body tracking focused primarily on outlining gestures driving hand tracking functionality, without clearly describing the underlying data collection processes (see Figure 2). The pop-up does not explain how

hand and body tracking work, or what data would be collected or accessible to third parties. As we observe in the Android context, it is challenging for users to make privacy decisions without being fully informed [44]; we are interested to explore the extent to which an understanding of device functionality drives or changes user permissions decisions.

3.3.2 The Quest 2 has demonstrated inconsistencies in permission protection level assignment. Namely, there is a lack of justification surrounding permission protection levels, and their downstream interpretation for the Quest 2. For example, we know that biometric data can be used to create privacy harms (see Section 2.1)—we want to understand why sensitive data types are being assigned normal permissions types. Relatedly, our investigation raises questions surrounding why body tracking was previously assigned a protection level of dangerous, and what motivated the change to a normal protection level. We are curious if these reassigned protection levels (and downstream consent implementations) are consistent with user perceptions of sensitivity.

3.3.3 The Quest 2 introduces non-traditional permissions flows. Lastly, all three biometric data types are controlled through similar-looking Settings toggles, using a novel implementation not drawn from the traditional Android permissions system. For head tracking, the toggle controls 6DoF vs 3DoF functionality globally across the device. For hand and body tracking, one toggle enables access to both data types across the device, without requiring later consent notifications. We are interested to assess the extent to which users understand this novel permission flow, which combines elements of AOSP normal and special permissions.

These observations motivate our subsequent interview study, which investigates how these permission flows shape user understanding of VR data collection and permissions behavior. In particular, we examine:

- whether users understand what biometric data types are collected in VR, when they are collected, and how they are collected;
- whether users understand the scope and meaning of these novel global permission flows; and
- whether immersive interaction modalities affect the effectiveness of traditional permission mechanisms.

4 RQ2 & RQ3 — Interview Study Methodology

To address the impact of our findings in Section 3 on users, we designed an interview study, which directly examines each of these differences introduced by the Quest 2 permissions system.

4.1 Interview Procedure

Our interview is divided into six parts, which we describe below. The general flow of our interview procedure is shown in Figure 3. Interviews lasted about 45 minutes.

Step 1: Relationship with VR. We began by asking participants to describe their previous experience with VR; namely, whether they own or have used a VR headset in the past, and if so, what types of applications they used. We sought to capture this information because we expected familiarity with VR technology, and Meta Quest devices specifically, may impact user mental models.

Step 2: VR tutorial. Next, we provide a tutorial on how to use the device (e.g., how to select objects or exit an app).

Step 3: App use. Then, participants use 5 popular VR applications for 3-5 minutes each; this allowed the user enough time to explore the app and experience the permission flow, without making the permission the user’s sole focus. We specifically chose not to indicate to participants that the study’s main focus was privacy and permissions to avoid social desirability bias. All participants used the same applications in the same order. Two applications requested microphone access, to capture the users’ voice, and two applications requested hand tracking, for interactivity. We selected these two biometric permissions because they are commonly supported by applications in the Quest store, and represent the two types of permissions flows that required user interaction: traditional pop-ups and system-wide toggles. Both applications which request microphone access present an AOSP-style pop-up to the user, as shown in Figure 6. For hand tracking, only the first application required the user to navigate to settings and turn on hand tracking, as shown in Figure 5, after which, hand tracking remained active. We used two applications with each permission type so we could prompt the participant with the first application as needed, and then assess whether users remembered the permission interaction or use within the second application without being prompted. This was particularly important for the hand tracking to investigate the new system toggle permission flow introduced on the Quest 2. We kept application ordering consistent, as we discuss further in Section 4.5.

As the user interacted with the application, we provided various instructions, (i.e., to search for a video in Youtube VR). We asked the participant periodically what they are seeing and doing, asking them to “think aloud” during this part of the study, so that we could capture how they reacted to the applications as they saw them.

The first application was the *Beat Saber Demo* [3]. This application is a coordination game where participants chop blocks using the controllers to the beat of a song. Beat Saber serves as a control, as it does not request any permissions from the user; we include a control to assess the participant’s general perceptions of VR data collection without prompts provided by the permissions system.

The next application was *Youtube VR* [6]. Like the traditional Youtube platform, Youtube VR hosts video content, with additional, immersive videos. During application use, we asked users to search for an immersive video of their choice, using the controllers to click and speech-to-text search feature to type. To do so, YouTube VR requests the microphone permission. This permission produces two traditional AOSP pop-ups, as shown in Figures 6 and 1. When the microphone is on, a passive indicator appears. Participants were then instructed to watch one video from the search results.

The third application was *Arkio* [2]. Arkio is a collaborative design platform, where users can create and discuss 3-D models together. During application use, we asked participants to initiate and join a meeting room. To do so, Arkio requests the microphone permission in the same manner as YouTube VR, shown in Figure 6. In Arkio, microphone use is a primary part of the user’s interaction with the application; while in Youtube VR, the user only used the microphone to record a search term, in Arkio, the user’s speech was accessed the entire time they were in the meeting room. There is similarly a passive indicator on screen during microphone use.

The fourth application was **MoveFast** [4]. MoveFast, like Beat Saber, is a coordination game, that focuses on aligning the user’s hand positions and movements to the screen, on the beat of a song. To do so, MoveFast requires the ability to track the users’ hands. When users initially open MoveFast, they are unable to use the app, as hand tracking is not enabled. We waited for the participant to ask for help (notice that the application was not allowing them to use controllers), at which point, we directed them to turn on hand tracking in Settings. This brings about a series of pop-ups, which show how to use hand tracking; one slide is shown in Figure 5. Generally, these pop-ups provided information about how hand tracking works, what data collection it requires, and how to use it. We did not directly tell participants they needed to read the text. The user then returns to the app, and continues on to gameplay. After gameplay, although we do not prompt them to do so, participants typically continued to use hand tracking to exit out of the app and did not disable the system-wide hand tracking.

The final application was **Richie’s Plank Experience** [5]. This application allows users to walk off the end of a plank at the top of a skyscraper. We asked users to first ride the elevator to the top of the building. This required them to push the elevator button with their finger, implicitly using hand tracking in their interaction with the application. Then we asked them to walk to the end of the plank (if they felt comfortable). The participant did not have to accept any permission to use hand tracking in this application, as it was already turned on at a system level when using the prior application. However, their hands were shown as being tracked throughout the game, and they used their hand to press the button in the elevator, triggering a visual indicator of the data collection, which has been previously shown to cause greater data collection awareness in Android [83]. We included this second application that features hand tracking to assess user’s perceptions of how hand tracking works across multiple apps.

Step 4: Data collection perceptions Next, we sought to understand how users perceive data collection in each of these applications—we wanted to identify whether participants understood the difference in scale and variety of data collection in VR (Diff #1 in Section ??). Therefore, for each application, we asked participants questions about (1) what data was collected, (2) how they think this data was collected, (3) why they think this data was being collected, and (4) how they think this data could be used. We also asked participants what drove their beliefs. We randomized the order in which we asked about each application to account for ordering effects, as participants were given more time to consider the data collection in latter applications.

Step 5: Perception of permissions model Next, we sought to understand how users interpret differences in permission request flows. As discussed in Section 3, the Meta Quest introduces different flows for sharing biometric data types; namely, some biometric data permissions must be turned on/off across the entire system. We asked questions to understand if users recalled permissions flows, and if users understood the meaning of permissions flows (i.e., the context and duration for which consent was being requested). We do so for both (1) a traditional Android permission request flow (e.g., the microphone permission flow) and (2) a new, Quest permission request flow (e.g., the hand tracking permission flow). We

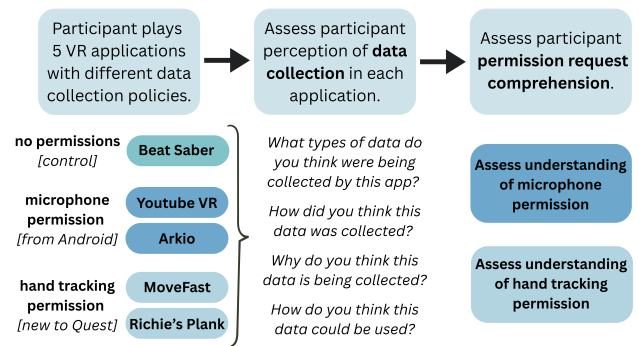


Figure 3: An overview of steps 3-5 of our interview procedure.

first prompted the participant, showing them the permission request from the first application with the given permission. We then asked participants what data type they believed the permission was requesting, and asked if they remembered any other applications using that data type. We then saw if the participant understood the second application also accessed the same data type, and if the participant understood why this was the case.

Step 6: Modality-specific privacy concerns Lastly, we explored whether users view modalities associated with the Meta Quest 2 as having greater privacy concerns than preceding technologies, such as Android devices. Specifically, we focus on understanding whether users think the same data policies should apply for hand tracking as for using a mouse or controller, and why. We believed this example was useful for several reasons; namely, it provides participants with a direct comparison with previous modalities, allowing them to frame their discussion in terms of *differences* between VR and preceding technologies, focusing in on novel privacy concerns. In particular, it allowed us to assess whether participants perceived behavioral biometric data collection as more sensitive than purely behavioral; in terms of data collection, each of these tracking types is increasingly invasive, and increasingly tied to biometrics.

Step 7: Demographic information Then, we asked participants to complete a Qualtrics survey with demographic questions (age, gender, race/ethnicity, education, and income), which we used to assess sample representativeness and to provide context for our results. We also asked questions from Gross et al.’s updated IUIPC survey [49] to assess general privacy perceptions and behaviors.

Step 8: Debrief We concluded each interview by informing participants about the study’s true focus and giving them the option of withdrawing their data from analysis.

4.2 Recruitment Procedure

We recruited 23 participants using flyers posted around two local universities. To avoid selection bias for participants most interested in privacy, our recruitment materials did not list privacy and permissions as the study’s focus, but instead framed the work as a study on VR generally. Participants submitted a Qualtrics survey, which contained study information and a consent agreement to participate, and scheduled a time to meet researchers in person via Google Calendar. Participants confirmed they were 18-65 years old and did not have any health conditions that put them at risk by using VR,

as defined by the Quest 2 Health and Safety Warnings [75]. Participants received a \$25 Visa gift card for their participation. Interviews were conducted between October and December of 2024.

4.3 Interview Analysis Procedure

To analyze interview responses, three researchers inductively developed an initial codebook by collaboratively coding three transcripts and reviewing the results among the full research team. Then, two research team members independently coded five interviews at a time, incorporating emergent codes and reducing redundancy based on agreement assessment and team discussion. We calculated inter-rater reliability (IRR) for each group of codes using Krippendorff's α [64]. We use Krippendorff's α as it provides a conservative measure accounting for chance agreements. Agreement was defined as both coders assigning an identical code to the same question response. After each round of coding, the two researchers met to discuss and resolve disagreements and update the codebook as necessary to capture new codes and refine codebook definitions. IRR was calculated per round to allow a staged approach, where a subset was double-coded before independently coding the remainder after reaching agreement, following best practice for assessing agreement in qualitative research [72]. We note one potential concern regarding IRR is that the rigid requirement for agreement could bias coding. However, this does not apply here as our interview data is already has a strict bounded structured due to the inherent nature of the interviewer-led in-lab interactions. This process was repeated for 4 rounds until an $\alpha > 0.8$ was achieved for each code, indicating strong agreement [64]. After coding all interviews, we conducted thematic analysis to identify trends across codes, following the recommendations of Braun and Clarke [28]. Our final codebook and α values for each code group are provided in our supplementary materials¹.

4.4 Participant Population

Detailed participant demographic information is shown in Table 1. We note our population was much younger and more male than the U.S. population. Consumer reports suggest the VR user base is also significantly younger and more male [59]; however, our participants were all under age 30, whereas a 2019 report indicating only 47% of VR users are under age 35 [56]. This population feature likely stems from our recruitment on a college campus; we discuss potential implications of this population in our limitations (Section 4.5) regarding age and education level. Our participants' privacy perceptions were in line with average student IUIPC scores from prior work [25, 91], with an average IUIPC score of 5.87.

When asked about any previous experience with VR, most participants indicated *limited* VR exposure (i.e., the participant had used a Google Cardboard before), but only four participants had *meaningful* previous experience with VR (i.e., the participant had played on a VR headset for more than 30 minutes in total). This is similar to estimates of the U.S. population—only 98 million people in the U.S. have ever used VR [1] (about 37% of the adult population). We discuss potential impact of VR exposure on user perspectives in both our results (Section 5.1) and limitations (Section 4.5).

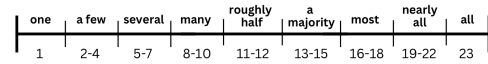


Figure 4: Our selected quantifier terminology

4.5 Limitations

Our study is limited by the size and demographics of our participant pool. Because we wanted to have participants interact with real-world systems, we structured our study as an in-person interview. The in-person nature of our study limited the participant pool we were able to recruit. Namely, our participant pool has limited age diversity, with all participants being under age 30—this is likely because our recruitment and study took place on a university campus, and most participants were likely university students. Therefore, our results may not generalize to older individuals, who may have less familiarity with technologies like VR or preceding technologies. However, it is likely changes to our population demographics would lead to a population with even greater misunderstandings beyond those of our results with our current population, as previous work suggests older age is associated with decreased digital literacy [37, 38]. It is possible that education or technical expertise may have shaped participants' interpretations of VR data collection—most of our participants self-reported that they were currently completing or had completed a university degree. It is also possible our study suffers from selection bias for people interested in VR. However, we note the general population of VR users are typically younger and more tech-interested adults [56]. Lastly, many participants had limited experience with VR devices, meaning our sample is likely more representative of new VR users. This is still valuable because people tend to make permission decisions early and rarely update them without prompting, so first impressions matter [10]. Additionally, people with substantial VR experience may actually be less representative of the broader population, as they are more likely to be technically knowledgeable early adopters. However, we note the lab setting may lead to behavior different from real-world use. For example, in the real-world, participants will use the Quest 2 in their own home, linked to personal accounts. This context may lead them to consider permissions differently. It is possible that more experienced users will have a more substantial frame of reference for privacy perspectives in the context of real-world use.

The interview-based nature of our study limited our ability to scale to a larger participant pool. While works such as Miller et al. [84] investigate hundreds of participants wearing VR headsets, the nature of the study, and of the qualitative analysis we undertake, is not feasible for a study at this scale. Additionally due to these time limitations, we only investigate a limited set of permissions. While the most recent Oculus Quest Pro devices incorporate face and eye tracking, this device is significantly more expensive, and has a smaller user base ownership. We believed focusing on permissions relevant to the Meta Quest 2 (i.e., hand tracking), would be most useful as initial work, especially as this permission introduced the most unique characteristics (e.g., new permissions flow, biometric data marked as "normal"). We recommend future authors investigate these additional biometric data types. We focus on the Meta Quest due to its popularity. While there exist other consumer

¹Our supplementary materials are available at https://osf.io/gw7v4/?view_only=cb2fd4451ff48f3801d220dbf106c6c

VR devices (i.e., the HTC Vive, Apple Vision Pro, Sony’s PSVR2), Meta’s market share of Q4 2024 VR device sales was 84% [92].

We further choose not to reorder application presentation across participants. We made this decision due to potential friction stemming from handing off controllers to and from participants between applications. Certain orderings may require excessive hand/controller transitions in a short period of time, drawing additional attention to the transition between hand/controller tracking in ways that are less representative of real-world use, leading to greater priming and more dramatic ordering effects. To minimize ordering effects associated with application ordering, we provided a refresher before discussing each application, to confirm participants recalled the correct interaction and application. We also grouped comparable applications—e.g., microphone apps were always both used and discussed consecutively. However, ordering effects may still have reduced recall for earlier permissions (i.e., the microphone), and improved understanding for later permissions (i.e., hand tracking). We believe this should not affect result fidelity, as we do not compare across permission and we will describe which permissions are at the per-permission level, with the exception of tracking recall in Section 5.1, where we specifically address the potential impact of these effects.

Additionally, we were only able to evaluate a limited set of applications; this was primarily due to the time limit of 30 minutes based on the recommendation of VR manufacturers [30]. However, we believe our selected applications represent a broad scope of the applications on the Meta Quest application store, consisting of entertainment, game, and productivity applications.

Lastly, it is possible participants provide more privacy-conscious responses than they would exhibit in practice due to social desirability bias. We attempt to address this by repeatedly reminding participants we are seeking honest user perspectives, and that there are not correct answers to questions we ask. We also chose not to tell participants the focus of our study was privacy and permissions until the end. Additionally, we gear our questions towards specific scenarios that occurred during the participants’ application use, or hypothetical scenarios based on the participants’ application use. For example, rather than directly asking “are you comfortable with hand tracking?”, we ask the participant “if there is a situation or circumstance where you would turn off hand tracking.”

4.6 Ethical Considerations

Our study was reviewed and approved by our institution’s ethics review board. Our primary ethical concerns surrounded participant safety and comfort during our study. We were careful to ensure study participants did not have medical conditions that would put them at risk by using a Meta Quest 2, and made sure to frequently check in with participants to ensure they were not experiencing discomfort. If they were experiencing discomfort, we took breaks during the study, and offered that participants could end their participation at any point, without loss of payment. We also took great measures to protect participant privacy; we used numerical identifiers to refer to participants in all records, including the consent process. Finally, because we used deception by not explicitly stating the focus of the study was on privacy, we debriefed participants at the end of the study about our true focus. We also gave participants

further information about the Android and Quest 2 permissions systems, and provided them the ability to withdraw if they were uncomfortable with the study’s true focus.

5 RQ2 & RQ3 – Interview Study Results

5.1 User Mental Models Regarding VR Data Collection

Our study provides insight into VR user mental models of data collection—specifically, the extent to which users understand what data types may be collected by each VR application, how this data is collected, and for what purpose. We further examine what drove these beliefs, to understand potential pathways for aligning user mental models with actual data collection, so users can make fully informed decisions when consenting to data collection. These findings may inform not only the design of the permissions system, but the structure of notice and choice frameworks more broadly. As this is a qualitative study, we report findings using *quantifier terminology* as defined in Figure 4 instead of raw counts, in line with previous work [12, 42, 51, 60].

Participants showed differing understandings of VR data collection, with some participants holding major misconceptions. When asked about data types collected by various applications, most participants noted that VR applications collect at least one new data type, such as head, body, or hand tracking. However, it became clear some participants did not understand how this biometric data was being collected.

After participants identified each data type, we asked them to tell us how they think the Meta Quest 2 collects this data. We also later specifically ask how participants think hand tracking works. In reality, hand tracking works using footage from the external cameras on the Meta Quest 2. Most participants correctly understood that there were sensors or cameras on the headset. Many of these participants believed hands were tracked using “sensors” broadly; for example, when asked how their hands were being tracked by the device, P11 stated, “There’s probably sensors in the eye, like, part of the headset... that tracks movement,” while P12 explained, “probably like external sensors underneath the headset.” However, a few participants provided answers that reflected fundamental misconceptions about the device’s functionality. For example, when asked the exact same question, P22 stated, “I was really shocked, because I wasn’t using controllers for this, so I’m just going to go with echolocation,” and P21 said, “Like, through my eyeballs? Right? Is that what you’re saying? Like, through my eyeballs?”.

It is clear many users did not have a complete understanding of how biometric data in VR is being collected. This is problematic because misconceptions surrounding how VR data collection works could lead users to underestimate data collection, and make misinformed privacy decisions. For example, in the context of hand tracking, knowing a camera is active all the time, as opposed to a motion sensor, may introduce greater privacy concerns.

Mental models of experienced VR users differentiated between immersive and non-immersive modalities. We observe participants who had previous experience with VR better understood how VR devices differed from preceding technologies, such

as Android devices. As discussed in Section 4.4, only four participants in our study had meaningful previous experience with VR. All experienced users identified privacy differences between the enhanced data collection occurring in VR and traditional modalities (i.e., mouse and controllers). For example, P4 stated, “in a somewhat privacy sense, it’s more intrusive to tracking a full hand [than a mouse],” and P6 explained, “I think just because of how tech is being integrated with like the human body, if they’re recording my hands they’re probably recording my general surroundings.”

Conversely, only a bit over half of participants without previous VR experience identified privacy differences between modalities. One participant equated the two, stating, “I think, like, if, yeah, now that you mentioned it, it’s probably, like, analogous to, like, a mouse” (P3), and another stated, “I think it’s the same, because if you’re holding the mouse, it’s also able to tell whether you’re fully holding it or not. So it’s already recording your hand” (P14). It is possible that increased context from repeated VR use may help users understand how VR works, and therefore potential privacy or differences between these modalities. However, it is also possible that these individuals are more interested in technology in general, since they own an emerging technology, and therefore have a better understanding of the privacy risks associated with VR. As the sample size of our study is limited, future work should investigate this effect, especially as VR use becomes more common.

While many participants recognize active tracking few discussed passive tracking. We define *active tracking* as data collection associated with a specific user interaction which triggers some user-presented application functionality. We thought of active tracking as VR actions that can be defined or replaced with a gamepad, such as with a Xbox controller. That is, instead of pressing a button on a controller (in the gamepad context), you “press” something in the virtual space with your finger. For example, in the MoveFast game, users are evaluated on their ability to punch or chop on the beat with a song. Therefore, when P7 stated that MoveFast was collecting, “movement data, tracking like, your punches and your palms,” we classified this data collection as active tracking. As we might expect, almost all participants recognized and discussed this type of tracking.

Conversely, we define *passive tracking* as any data collection not directly tied to an action-triggering user interaction. Passive tracking is occurring at all times in VR; cameras are used throughout device use to track user surroundings and movement. We believe this passive tracking is much more invasive than active tracking, due to its duration. P15 described this type of tracking, saying, “you can guess where the rest of the body is based on if you’re crouching, leaning, I feel you can get actually pretty good information about how people’s bodies move from that.”

However, only a few participants acknowledged passive tracking outside of the context of app interactions. It appears participants only considered tracking in the context of their active interactions with the applications, despite the presence of passive indicators of bodily tracking in the frame (e.g., depictions of their hands shown when their hands were in the frame). An understanding of passive tracking is key to understanding VR’s increased invasiveness; without understanding the extent of collection, users may underestimate the data they are consenting to having collected.

It is worth noting that, as discussed in Section 4.5, an ordering effect may be present surrounding tracking recall—meaning that participants were less likely to recall earlier experiences (i.e., applications using the microphone). Our results are contrary to this expected effect as participants more often recalled active tracking (microphone) over passive tracking (hand tracking), which was the second type of tracking shown.

Participants derived data collection mental models from interaction and previous technology, in addition to permissions pop-ups. Previous work around Android smartphone permissions has demonstrated that data collection interactions are more memorable when they are directly tied to the interactions taking place in the application [83]. We observe this behavior in our immersive modality as well. In the context of hand tracking, when we asked participants to list the data types they think were collected by each app, we see most participants listed hands for MoveFast. In MoveFast, users primarily interact using their hands. Compared with MoveFast, less than half as many participants identified hand tracking in the context of Richie’s Plank. The only use of hand tracking use in Richie’s Plank is to realistically display the users hands as they survey and press the elevator button one time during the interaction. Hand tracking could be removed without significantly impacting the experience. Similarly, for Beatsaber, where participants used light sabers (controllers) to slash objects, most participants listed controllers, whereas in Youtube VR, where the controllers were only used to click on the search bar and to find a video, only a few participants listed controller data as a collected data type.

We saw similar behavior surrounding the microphone permission as well. For Arkio, the virtual meeting application, many participants correctly recalled the microphone was requested. However, for Youtube VR, a video player, where the microphone is not a primary part of the application’s purpose, half as many participants correctly recalled that the microphone was requested. It appears that relevance to application functionality is more important than passive indicators (as present in Youtube and Arkio), which were less of a driver of user permission recall.

When incorrect data types were listed, they were consistently associated with application functionality. For example, when users suggested that heart rate data were collected by the Richie’s Plank app: “I think I’ve seen other games... track heart rate through controllers... so it could be like, I don’t know, something through the head, temples wherever. Or there’s a vein so people can just check if the blood’s pumping” (P20). This application entailed walking on a plank above a skyscraper, which would probably cause increased heart rate and stress. Participants seem to consider the functionality of the app as an initial step towards hypothesizing data types that may have been collected.

A majority of participants cited previous technologies as guiding their thinking surrounding data collection and permissions interactions. In some instances, these were helpful metaphors. For example, P11 compared Youtube’s passive indicator to indicate microphone usage as similar to their tablet: “when using the mic on your tablet, you see a light.” Additionally, privacy concerns from previous technology drives perception of data collection in VR as

well. Several comparisons to previous technology centered on concerns surrounding advertising and third party sharing. Notably, participants expressed fairly severe distrust in Meta, stemming from their prior behavior. For example, P4 stated, “I also know how aggressive Meta is, so I know... at least I think they’ll also track the pass through and see if that helps them,” and expressed that “Meta is really bad with data, in terms of privacy.” Similarly, P20 suggested a smaller application could not record outside the application unless they had “backdoor deals with Facebook.” It appears participants’ negative perception of Meta’s data practices may negatively impact perceptions of data collection throughout device use, despite Meta only owning the platform, and not owning any of the assessed applications on which we focused our study.

5.2 User Understanding of AOSP Permissions Flows

Next, we examine participant understanding and recall of the microphone permission pop-up, which was our example of a traditional AOSP permission flow. Specifically, we considered whether the new, immersive modality surfaced unique issues which had not been observed in prior smartphone privacy work.

Participants correctly understood what the microphone pop-up gave access to, and recalled collection. We presented participants with a copy of the microphone pop-up that participants accepted during their use of Youtube VR. We asked participants what data they thought they were agreeing to share, and all participants correctly understood the application was requesting access to the microphone. After discussing the YouTube permission pop-up, we asked participants if they recalled any other applications that could record their microphone. A majority of participants were able to correctly recall that Arkio accessed the microphone.

However, participants had varying perceptions of how long the microphone could record. We further asked participants under what circumstances microphone access would be shared with the application. We specifically asked the duration of time that the participant thought the application would be able to record their microphone. The participants gave mixed responses about recording duration. Of the participants who provided a response, many believed an application could access the microphone at any time while the application is being used. This perception is correct as recent versions of AOSP used by Quest 2 restrict sensitive permission access to only be possible when using the app. A few participants believed the microphone could be accessed until the user closed the application for the first time since accepting the permission; for example, P20 stated the microphone is able to record, “probably until, like, the computer goes to sleep or shuts down.”

Many participants believed applications could only access the microphone when prompted (e.g., when the user presses the microphone button), underestimating possible data collection. Some of these participants tied the end of the recording to in-application actions: “I think they were more just, you know, activated just when I was searching through the search bar and then hopefully, well, I’m hoping at least, when I actually played the video, they stopped it” (P4). Others set hard time limits on how long the microphone recorded, stating, “I don’t know, two hours,

three hours?” for Arkio (P18) or “I would guess it would be at most 10 seconds” for YouTube (P3). Alternatively, two users believed the application could record both while the application is used and not being used, confirming that they believed if “you exit the app, it would still be recording” (P22). We note this last perspective was true in older versions of Android, i.e., before Android 11 was released in 2020. In these older versions, the microphone could be accessed while the application was in the background [39].

Participants incorrectly assumed microphone recording capability would be restricted to the applications’ specific context of use. For example, when asked the same question about potential recording duration in both YouTube and Arkio, P9 indicated that Youtube “can only record my microphone when I press the microphone button until when I click search,” and minutes later when discussing Arkio, they stated “as long as you’re in the [meeting] room and you have multiplayer turned on they would have the microphone on.” Although apps ideally access sensitive resources only as needed, the permission system permits broader access.

5.3 User Understanding of Novel Permissions Flows

Lastly, we examine participant understanding and recall of the global permission flow for hand tracking, which was newly added by the Meta Quest. We sought to understand what features drive user comprehension and comfort with this new permission flow.

Participants understood hand tracking was a global permission because it was located in the system settings page. The big change for this permission flow introduced on the Meta Quest 2 is that hand tracking is turned on and off at the system level. That is, if you enable the permission, it is enabled for all applications. This is explained to users when they enable the permission as they are forced to navigate to the settings page, which provides text indicating the global nature of the permission. However, prior work has shown users do not always read these types of pop-ups [23].

We found the Meta Quest’s approach appears quite successful; nearly all participants correctly interpreted this permission flow. As P6 correctly inferred, “I had to go into the settings and click like the toggle switch [to turn on hand tracking]. I would assume that that’s not going to go off unless I manually turn it off.” When participants were asked to explain how they knew the permission spanned across applications, nearly all stated they knew this was a global permission because they had to change a device-wide setting. For example, P13 said, “because this one was in the settings of the actual platform, as opposed to the actual app.”

This is interesting, because in the context of microphone permission request, few participants referenced the permission request when we asked participants how they knew Arkio could access the microphone, despite having just discussed this pop-up in relation to YouTube microphone access. Instead, many other participants referenced the application functionality as the reason they were aware Arkio accessed the microphone. For example, P9 stated, “to use the room voice chat multiplayer you need to have the microphone to be able to chat with other people”. While it is possible that people mention the application functionality instead of the popup because it is more natural to discuss, the contrast between the responses suggests the hand-tracking permission flow might be

more memorable, given that functionality related indicators were present in both permissions flows.

Participants acknowledged usability benefits of a global hand tracking permission. When asked if the settings-based global permission flow was appropriate for controlling access to hand tracking data, users implicitly discussed the privacy-utility trade-off. Roughly half of participants stated the global permission was likely in place to make things easier for the user, i.e., avoiding potentially annoying repeated access requests. As P4 explained, “a user might be pissed off just because you keep asking them the same thing over and over, especially when they’re new to this, and then, in this case, you know, asking you to go to different apps in a period of time, that might really cause the user to be frustrated.” Another participant (P2) added, “I think it’s a good matter of convenience.”

However, participants were also concerned with potential privacy overreach stemming from a global hand tracking permission. Roughly half of the participants also acknowledged the potential privacy loss with this approach. A few participants explicitly weighed the trade-off between privacy and utility, stating, “This becomes more of an ethic question, where my gut feeling would generally say no [regarding turning on hand tracking], just because I know it’s like privacy-wise, I shouldn’t be giving up my privacy, right? But that’s at the same time, and especially with Meta’s privacy terms and conditions, I know that if I don’t allow that, then I don’t really have any other choice but not to use the product itself, right? So if I actually enjoy the product, I wanna use the product, that’s something I have to trade off,” (P4) and, “If it popped up every single time you wanted to use it, it could get tedious and annoying. So they just have it show up once. But it can be, I guess, a problem if you just forget that you turned it on, and it’s collecting data that you don’t want it to” (P14).

Lastly, a few participants stated they were comfortable with this trade-off, but just for hand tracking data specifically. They said they would be more concerned if it focused on a different data that they viewed as more sensitive. As an example, P5 said, “I think it’d be less comfortable if it was like with the voice”; they justified this belief because they viewed voice data as something that “you can use rather than like hands” (P5); the participant did not foresee potential harms stemming from hand tracking data.

Participants suggested potential alternative mechanisms for a hand tracking permission flow, which provide more fine-grained user control. While we did not explicitly ask participants to provide more appropriate alternative mechanisms, a few who saw potential issues with the current mechanism offered proposals, which were centered on providing more notice to users regarding the data collection’s scope of data on a per-app basis. For example, P16 suggested users should be given different options for the permission, to determine whether you “want to be asked only once or several times.” Similarly, P11 suggested a per-app toggle, stating, “I don’t know why [the request] only takes place once. It should probably be for every game. Or, you can have a setting where you can turn it on for every game. Because, for websites, you can allow access to the microphone for one site, but the next site won’t assume that you want the microphone.” Lastly, P22 said they “wish there was a button to turn it off immediately after I’m done playing.”

We further discuss the feasibility and utility trade-offs surrounding these proposals in Section 6.

Many participants who were comfortable with the global approach bucket their privacy concerns across applications. They felt if they were to allow hand tracking for one application, they would likely allow it for all applications anyway. For example, P6 stated, “They’re tracking different things, but like I’m acknowledging that they are tracking something. But if I don’t want to be tracked, I’ll just turn it off across the board.” Similarly, P7 said, “It’s like, oh, you allowed it for one app, then you’re going to probably allow it for every other app.” This belief aligns with Meta’s permissions flow implementation, where the permission is granted at the device level. It is interesting to consider whether participant preference is the best metric for designing a permissions system—we further discuss the implications of this approach in Section 6.

6 Discussion

We must consider how data collected in VR, and its potential downstream use, ought to drive notice and choice frameworks for VR privacy. In this study, we examine user understanding of the Meta Quest 2’s permission system. Based upon demonstrated misconceptions possessed by participants, we provide several suggestions for Meta system developers, VR application developers, and HCI researchers, to establish more effective permissions systems and privacy notices for VR devices.

Meta should introduce implicit cues and experiences to help new users understand the scope of data collection in VR. In Android, biometric data permissions are categorized as ‘dangerous’ and require users to consent for collection at runtime [14]; the Quest 2, however, does not use a purely run-time permissions system, but often relies upon a hybrid approach for biometric data, where implicit authorization is provided for all applications at one time. This approach of implicit authorization is supported by participants for the VR setting; despite the potential ‘dangers’ of biometric data, it is frequently required for functionality, and users would likely grow frustrated or discount frequent warnings. We find, at a high level, users understood each permission we examine: they recognized the traditional pop-up requested access to the microphone, and that the hand tracking toggle allowed all applications to track the position of their hands. However, users lacked a deeper level of understanding; for example, under what circumstances applications can access the microphone, or the nature of how, and how precisely, hands are tracked. This was particularly true for inexperienced VR users, who had difficulty differentiating Quest 2 data from that of preceding technologies.

To address this issue in the context of microphone usage, our findings support an approach based on system-enforced consistent passive indicators (e.g., an icon symbolizing the microphone being turned on), as our study participants frequently referenced passive indicators as useful when determining permissions scope. This additionally aligns with the findings of previous work in the Android space, which examines the extent to which an “explicit foreground visual indicator of use” increases participant comfort with data collection [109]. In the context of hand tracking, we believe that providing users with greater intuition surrounding *how* hand tracking works (i.e., by analyzing camera data) will allow

users to make more informed decisions. Meta could explore the use of required and prominent skeletons to draw attention to body tracking, to make it clear what exactly is being tracked. Similarly, Meta could explore using passthrough (when the headset displays the user's surroundings) for the duration of the hand tracking tutorial, so that users directly comprehend their hands are being tracked using cameras, or provide more interactive tutorials about *what data is necessary* to make hand tracking work, rather than just how hand tracking works. One participant noted that briefly seeing passthrough (when they stepped outside a boundary) made them recall the device uses cameras; incorporating direct use of modalities into tutorials will increase data collection clarity.

Third-party applications should use in-app interactions to help users understand the scope of permissions in VR. Third-party applications should take steps to improve users' understanding of data collection and use. In particular, they should be transparent about passive tracking, especially with newer biometric data types such as hand and body tracking. We found most users recognized biometric tracking when it was directly part of gameplay. Accordingly, applications should integrate collected data types into core functionality. During startup, applications could include a brief interaction using the relevant data type to make collection explicit.

Mechanisms for more fine-grained control over hand tracking should be explored, focusing on the trade-off between privacy and usability. The immersive modality of VR introduces a new aspect to the tradeoff between usability and privacy in the context of permissions, adding increased challenges to implementing an app-by-app permissions framework. In VR, hand tracking is a truly global permission—when users exit the app, their hands are tracked and used by the system to navigate menus, open applications, etc. This adds an interesting dimension to how we should think about the permission; not only do we have to consider data access being granted to the device operator (e.g., Meta), we also must consider the usability aspects of this difference. If a user is navigating an application using their hands, and then goes to open a new application, and suddenly finds themselves unable to use their hands, this would likely be disorienting, or annoying at best.

One possible solution is to let users navigate the privacy-usability trade-off for themselves. As examined in Section 5.3, a few participants provided suggestions for how they would like to be prompted for data access; for example, offering proposals where users make a global choice as to whether they would like to be prompted for every application, or users are simply able to toggle on/off for individual applications, even if all are turned on at first. Presenting biometric data permissions in an accessible and descriptive manner will allow users to align their behavior with their privacy preferences.

VR platforms need to update traditional notice and choice frameworks to better fit this immersive modality. Our results demonstrate that users hold significant misunderstandings about data collection in VR and often fail to grasp the scope, mechanisms, and types of tracking involved. Although not sufficient for broad generalization, our findings suggest more experienced users may have better intuition about VR data collection practices. This points to potential changes that could improve traditional notice-and-choice frameworks. For example, conventional approaches such as AOFU or one-time opt-in/opt-out mechanisms may be poorly suited

to immersive modalities. These models assume that a single decision (made when a feature is first encountered) can reliably reflect a user's ongoing preferences. However, in VR and other immersive environments, users often begin interactions with limited familiarity, and may not fully understand the implications of opting in to a particular form of data collection or granting a permission. Relying on one-time prompts may lock users into choices that no longer reflect their evolving comfort levels, expectations, or awareness as they gain experience with immersive technologies. Future work will be needed to investigate the relationship between VR experience, users' understanding of permissions, and their preferences surrounding prompting.

Future researchers should examine the impact of new features introduced by the Quest 3, and other popular consumer devices. Since this study took place, the Quest 3 has emerged as a popular consumer VR device; it is therefore worth considering how our findings may generalize to this new device. We hypothesize that our findings likely will extend to the Quest 3. The primary change on the Quest 3 is the incorporation of improved sensors, which permit color passthrough (vs. Quest 2's black-and-white passthrough), and allow for more in-depth body tracking. Though it appears the Quest 2 and 3 have similar UX designs, it is possible color passthrough may increase user awareness of camera-based tracking by presenting a more realistic environment.

Similarly, we believe that the bulk of our findings will generalize to VR devices more broadly. Biometric data collection is similar across devices (i.e., most consumer devices use cameras and IMUs to track users); our findings surrounding mental models (Section 5.1) will likely also be broadly applicable. The permissions flows we examine and discuss in Section 5.3 are broad, and are likely to represent a bulk of flows that will be seen on other VR devices; however, we believe it will be important for future work to examine the extent to which implementations differ between the Quest 2 and other future devices, and the impact on user understanding.

Future researchers should examine the perspectives of a broader scope of demographics. Our study primarily interviewed university-aged participants with minimal VR exposure, it is possible that this demographic characteristic may have impact user privacy perspectives surrounding VR. We did observe potential differences based upon users' previous experience with VR, but we did not have a sufficient sample to make generalizable claims regarding those comparisons. We suggest that future researchers examine a broader demographic participant sample, to better understand the impact of characteristics such as age, tech-forwardness, VR experience, and education on user perspectives surrounding VR privacy.

References

- [1] 2023. AR & VR Adoption Is Still in Its Infancy. <https://www.statista.com/chart/28467/virtual-and-augmented-reality-adoption-forecast>.
- [2] 2025. Arkio. <https://www.meta.com/experiences/arkio/2280319701979278/>. Online; accessed November 2025.
- [3] 2025. Beat Saber - Demo. <https://www.meta.com/experiences/beat-saber-demo/1758986534231171/>. Online; accessed November 2025.
- [4] 2025. MoveFast. <https://www.meta.com/experiences/move-fast/6087525674710349/>. Online; accessed November 2025.
- [5] 2025. Richie's Plank Experience. https://www.meta.com/experiences/pcvr/richies-plank-experience/1388204261277129/?srsltid=AfmBOoolylDquaj5Ngb7aB5r_dRoWbHQEHgYCN-J28zWy04WwZDrzeUE. Online; accessed November 2025.

- [6] 2025. Youtube. <https://www.meta.com/experiences/youtube/2002317119880945/>. Online; accessed November 2025.
- [7] Melvin Abraham, Mark McGill, and Mohamed Khamis. 2024. What You Experience is What We Collect: User Experience Based Fine-Grained Permissions for Everyday Augmented Reality. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–24.
- [8] 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.
- [9] Efthimios Alepis and Constantinos Patsakis. 2019. Unravelling security issues of runtime permissions in android. *Journal of Hardware and Systems Security* 3 (2019), 45–63.
- [10] Hazim Almuhammedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your location has been shared 5,398 times! A field study on mobile app privacy nudging. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. 787–796.
- [11] Brooke Altman. 2019. A Product Designer's Reflections on HTC Vive and Oculus Quest. <https://medium.com/@baltman/a-product-designers-reflections-on-htc-vive-and-oculus-quest-ea2966af7789>
- [12] Sabrina Amft, Sandra Höltervennhoff, Rebecca Panskus, Karola Marky, and Sascha Fahl. 2024. Everyone for themselves? a qualitative study about individual security setups of open source software contributors. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1065–1082.
- [13] Android Code Search. 2023. AndroidManifest.xml. <https://cs.android.com/android/platform/superproject/+/master:frameworks/base/core/res/AndroidManifest.xml>. Online; accessed 1 Dec 2023.
- [14] Android Developers. 2023. Permissions on Android. <https://developer.android.com/guide/topics/permissions/overview>. Online; accessed 1 Dec 2023.
- [15] Android Developers. 2023. Request special permissions. <https://developer.android.com/training/permissions/requesting-special>. Online; accessed 1 Dec 2023.
- [16] Android Developers. 2024. Sensors Overview. https://developer.android.com/develop/sensors-and-location/sensors/sensors_overview. Online; accessed 1 November 2024.
- [17] Android Developers. 2025. *Motion Sensors*. https://developer.android.com/develop/sensors-and-location/sensors/sensors_motion Accessed: 2025-05-19.
- [18] Android Developers. n.d. Permissions. <https://stuff.mit.edu/afs/sipb/project/android/docs/guide/topics/security/permissions.html>. Accessed: 2026-05-12.
- [19] Android Help. 2023. Change app permissions on your Android phone. <https://support.google.com/android/answer/9431959?hl=en>. Online; accessed 1 Dec 2023.
- [20] Android Source. 2023. Android Open Source Project. <https://source.android.com>. Online; accessed 1 Dec 2023.
- [21] ARTillery Intelligence. 2023. VR Usage & Consumer Attitudes, Wave 8. <https://artilleryiq.com/reports/vr-usage-consumer-attitudes-wave-8/>. Online; accessed Nov 2024.
- [22] Hamid Bagheri, Eunsuk Kang, Sam Malek, and Daniel Jackson. 2018. A formal approach for detection of security flaws in the android permission system. *Formal Aspects of Computing* 30 (2018), 525–544.
- [23] G Susanne Bahr and Richard A Ford. 2011. How and why pop-ups don't work: Pop-up prompted eye movements, user affect and decision making. *Computers in Human Behavior* 27, 2 (2011), 776–783.
- [24] David G Balash, Mir Masood Ali, Chris Kanich, and Adam J Aviv. 2024. "I would not install an app with this label": Privacy Label Impact on Risk Perception and Willingness to Install {iOS} Apps. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. 413–432.
- [25] David G Balash, Dongkun Kim, Darika Shaibekova, Rahel A Fainchtein, Micah Sherr, and Adam J Aviv. 2021. Examining the Examiners: Students' Privacy and Security Perceptions of Online Proctoring Services.
- [26] Rainer Böhm and Jens Grossklags. 2011. The security cost of cheap user interaction. In *Proceedings of the 2011 New Security Paradigms Workshop*. 67–82.
- [27] Alex Bowyer, Jack Holt, Josephine Go Jefferies, Rob Wilson, David Kirk, and Jan David Smeddinck. 2022. Human-GDPR interaction: practical experiences of accessing personal data. In *Proceedings of the 2022 CHI conference on human factors in computing systems*. 1–19.
- [28] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. <https://doi.org/10.1191/1478088706qp0630a> arXiv:https://doi.org/10.1191/1478088706qp0630a
- [29] Gavin Buckingham. 2021. Hand tracking for immersive virtual reality: opportunities and challenges. *Frontiers in Virtual Reality* 2 (2021), 728461.
- [30] Business Insider. 2018. *Virtual Reality Side Effects*. <https://www.businessinsider.com/virtual-reality-vr-side-effects-2018-3#seizures-3> Accessed: 2026-05-14.
- [31] Paolo Calciati, Konstantin Kuznetsov, Alessandra Gorla, and Andreas Zeller. 2020. Automatically granted permissions in Android apps: An empirical study on their prevalence and on the potential threats for privacy. In *Proceedings of the 17th International Conference on Mining Software Repositories*. 114–124.
- [32] Jiaxun Cao, Anupam Das, Pardis Emami-Naeini, et al. 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, 1554–1572.
- [33] Weicheng Cao, Chunqiu Xia, Sai Teja Peddinti, David Lie, Nina Taft, and Lisa M Austin. 2021. A large scale study of user behavior, expectations and engagement with android permissions. In *30th USENIX Security Symposium (USENIX Security 21)*. 803–820.
- [34] Kaiming Cheng, Arkaprabha Bhattacharya, Michelle Lin, Jaewook Lee, Aroosh Kumar, Jeffery F Tian, Tadayoshi Kohno, and Franziska Roesner. 2024. When the User Is Inside the User Interface: An Empirical Study of UI Security Properties in Augmented Reality. In *USENIX Security Symposium*.
- [35] Lorrie Faith Cranor. 2012. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J. on Telecomm. & High Tech. L.* 10 (2012), 273.
- [36] James J Cummings, Alexis Shore Ingber, and Yihan Danny Jia. 2025. Self-Disclosure in Social Virtual Reality: The Influence of Information Management Dynamics, Social Presence, and Privacy Concerns. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. 1–16.
- [37] Sara J Czaja, Neil Charness, Arthur D Fisk, Christopher Hertzog, Sankaran N Nair, Wendy A Rogers, and Joseph Sharit. 2006. Factors predicting the use of technology: findings from the Center for Research and Education on Aging and Technology Enhancement (CREATE). *Psychology and aging* 21, 2 (2006), 333.
- [38] Sara J Czaja and Joseph Sharit. 1998. Age differences in attitudes toward computers. *The Journals of Gerontology Series B: Psychological Sciences and Social Sciences* 53, 5 (1998), P329–P340.
- [39] Android Developers. 2025. Foreground services in Android 11. <https://developer.android.com/about/versions/11/privacy/foreground-services>. Online; accessed May 2025.
- [40] Android Developers. 2025. Request special permissions. <https://developer.android.com/training/permissions/requesting-special>. Online; accessed May 2025.
- [41] Meta Developers. 2025. Body Tracking for Movement SDK for Unity. <https://developers.meta.com/horizon/documentation/unity/move-body-tracking/>. Online; accessed May 2025.
- [42] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring how privacy and security factor into IoT device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.
- [43] Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, and David Wagner. 2011. Android permissions demystified. In *Proceedings of the 18th ACM conference on Computer and communications security*. 627–638.
- [44] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the eighth symposium on usable privacy and security*. 1–14.
- [45] Yuan Yuan Feng, Yaxing Yao, and Norman Sadeh. 2021. A design space for privacy choices: Towards meaningful privacy control in the internet of things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–16.
- [46] Google. 2025. [frameworks/base/core/res/AndroidManifest.xml](https://cs.android.com/android/platform/superproject/+/master:frameworks/base/core/res/AndroidManifest.xml). <https://cs.android.com/android/platform/superproject/+/master:frameworks/base/core/res/AndroidManifest.xml>. Online; accessed September 2025.
- [47] Sindhu Reddy Kalathur Gopal, Diksha Shukla, James David Wheelock, and Nitesh Saxena. 2023. Hidden reality: Caution, your hand gesture inputs in the immersive virtual world are visible to all! In *32nd USENIX security symposium (USENIX Security 23)*. 859–876.
- [48] Colin M Gray, Cristiana Santos, Nataliia Bielova, Michael Toth, and Damian Clifford. 2021. Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. In *Proceedings of the 2021 CHI conference on human factors in computing systems*. 1–18.
- [49] Thomas Groß. 2020. Validity and Reliability of the Scale Internet Users' Information Privacy Concern (IUIPC)[Extended Version]. *arXiv preprint arXiv:2011.11749* (2020).
- [50] Hanyang Guo, Hong-Ning Dai, Xiapu Luo, Zibin Zheng, Gengyang Xu, and Fengliang He. 2024. An Empirical Study on Oculus Virtual Reality Applications: Security and Privacy Perspectives. In *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*. 1–13.
- [51] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2020. "It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–12.
- [52] 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 2024 CHI Conference on Human Factors in Computing Systems*. 1–24.
- [53] David Harborth and Alisa Frik. 2021. Evaluating and redefining smartphone permissions with contextualized justifications for mobile augmented reality

- apps. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 513–534.
- [54] Scott Hayden. 2024. Quest 2 and Quest Pro are Being Discontinued, Encouraging Wider Adoption of Mixed Reality. <https://www.roadtovr.com/quest-2-pro-discontinued-quest-3s-release-mixed-reality/>
- [55] David Heaney. 2020. *Oculus Firmware Reveals New Touch Controllers, Referencing Improvements To Tracking, Finger Sensing, Haptics*. <https://www.uploadvr.com/oculus-jedi-controller-driver-found/> Accessed: 2025-05-19.
- [56] Greenlight Insights. 2019. 2019 Virtual Reality Consumer Report. <https://greenlightinsights.com/reports/2019-virtual-reality-consumer-report/>
- [57] Ismat Jarin, Yu Duan, Rahmadi Trimananda, Hao Cui, Salma Elmalaki, and Athina Markopoulou. 2023. Behavr: User identification based on vr sensor data. *arXiv preprint arXiv:2308.07304* (2023).
- [58] Emiram Kablo, Melina Kleber, and Patricia Arias Cabarcos. 2025. {PrivaCI} in {VR}: Exploring Perceptions and Acceptability of Data Sharing in Virtual Reality Through Contextual Integrity. In *34th USENIX Security Symposium (USENIX Security 25)*. 1531–1548.
- [59] Jasmine Katatikarn. 2025. Virtual Reality Statistics: The Ultimate List in 2024. <https://academyofanimatedart.com/virtual-reality-statistics/>
- [60] Harjot Kaur, Carson Powers, Ronald E Thompson III, Sascha Fahl, and Daniel Votipka. 2025. “Threat modeling is very formal, it’s very technical, and also very hard to do correctly”: Investigating Threat Modeling Practices in Open-Source Software Projects. In *34th USENIX Security Symposium (USENIX Security 25)*.
- [61] Patrick Gage Kelley, Joanna Breese, Lorrie Faith Cranor, and Robert W Reeder. 2009. A “nutrition label” for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*. 1–12.
- [62] Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. 2012. A conundrum of permissions: installing applications on an android smartphone. In *Financial Cryptography and Data Security: FC 2012 Workshops, USEC and WECSR 2012, Kralendijk, Bonaire, March 2, 2012, Revised Selected Papers 16*. Springer, 68–79.
- [63] Simon Koch, Benjamin Altpeter, and Martin Johns. 2023. The {OK} is not enough: A large scale study of consent dialogs in smartphone applications. In *32nd USENIX Security Symposium (USENIX Security 23)*. 5467–5484.
- [64] Klaus Krippendorff. 2011. Computing Krippendorff’s alpha-reliability.
- [65] Lin Kyi, Sushil Ammanaghatta Shivakumar, Cristiana Teixeira Santos, Franziska Roesner, Frederike Zufall, and Asia J Biega. 2023. Investigating deceptive design in GDPR’s legitimate interest. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–16.
- [66] Steven M LaValle, Anna Yerushova, Max Katsev, and Michael Antonov. 2014. Head tracking for the Oculus Rift. In *2014 IEEE international conference on robotics and automation (ICRA)*. IEEE, 187–194.
- [67] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. 2017. Securing augmented reality output. In *2017 IEEE symposium on security and privacy (SP)*. IEEE, 320–337.
- [68] Rui Li, Wenrui Diao, Zhou Li, Jianqi Du, and Shanqing Guo. 2021. Android custom permissions demystified: From privilege escalation to design shortcomings. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 70–86.
- [69] Jonathan Liebers, Sascha Brockel, Uwe Gruenefeld, and Stefan Schneeeggass. 2024. Identifying users by their hand tracking data in augmented and virtual reality. *International Journal of Human-Computer Interaction* 40, 2 (2024), 409–424.
- [70] Jialiu Lin, Bin Liu, Norman Sadeh, and Jason I Hong. 2014. Modeling {Users’} mobile app privacy preferences: Restoring usability in a sea of permission settings. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. 199–212.
- [71] Aleecia M McDonald and Lorrie Faith Cranor. 2008. The cost of reading privacy policies. *Isjlp* 4 (2008), 543.
- [72] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 72 (Nov. 2019), 23 pages. <https://doi.org/10.1145/3359174>
- [73] Richard McPherson, Suman Jana, and Vitaly Shmatikov. 2015. No escape from reality: Security and privacy of augmented reality browsers. In *Proceedings of the 24th international conference on world wide web*. 743–753.
- [74] Meta. 2023. Hand and Body Privacy Notice. <https://www.meta.com/ca/legal/quest/hand-tracking-privacy-notice/>. Online; accessed May 2025.
- [75] Meta. 2025. Health & Safety Warnings. <https://www.meta.com/legal/quest/health-and-safety-warnings/?srsltid=AfmBOop3quini03brwv2NWe9f1eXyGp7J1oNiTcQnCsAXrdVUTaxs89M>. Online; accessed May 2025.
- [76] Meta. 2025. Learn about Hand and Body Tracking on Meta Quest. https://www.meta.com/help/quest/29014772643252/?srsltid=AfmBOoqFJFv_KxtAYj1ZNYSYnPhh9l_kZE5npGm3PboMx7YF7ZngxeER. Online; accessed May 2025.
- [77] Meta. 2025. Learn how headset tracking works on Meta Quest. https://www.meta.com/help/quest/598701621088668/?srsltid=AfmBOopgpOUEDqgt_9ysU_gyhJyaocYgV4hG0Ab2Mchb9Ml9ooQcErWjE. Online; accessed May 2025.
- [78] Meta Horizon Developers. 2024. *Hands Setup*. <https://developers.meta.com/horizon/documentation/unity/unity-handtracking-hands-setup> Accessed: 2025-05-19.
- [79] Meta Platforms, Inc. 2026. *Body Tracking in Native Android Applications*. <https://developers.meta.com/horizon/documentation/native/android/move-body-tracking/> Meta Horizon Developers Documentation, accessed May 18, 2026.
- [80] Meta Platforms, Inc. 2026. *Create Body Tracker — Meta Horizon Developers Documentation*. <https://developers.meta.com/horizon/documentation/native/android/move-body-tracking/#create-body-tracker> Accessed May 18, 2026.
- [81] Meta Quest Blog. 2013. Building a Sensor for Low Latency VR. <https://www.meta.com/blog/quest/building-a-sensor-for-low-latency-vr/>. Online; accessed 1 November 2024.
- [82] Abraham Mhaidli, Selin Erin Fidan, and Florian Schaub. 2025. Intriguing, Concerning, and Questioning the Impact on Immersion: An Exploration of VR Users’ Advertising Experiences and Attitudes. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. 1–19.
- [83] Kristopher Micinski, Daniel Votipka, Rock Stevens, Nikolaos Kofinas, Michelle L Mazurek, and Jeffrey S Foster. 2017. User interactions and permission use on android. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 362–373.
- [84] 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. *Scientific Reports* 10, 1 (2020), 17404.
- [85] 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. In *32nd USENIX Security Symposium (USENIX Security 23)*. 895–910.
- [86] Anh Nguyen, Xiaokuan Zhang, and Zhisheng Yan. 2024. Penetration vision through virtual reality headsets: Identifying 360-degree videos from head movements. In *33rd USENIX Security Symposium (USENIX Security 24)*. 2779–2796.
- [87] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.
- [88] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI conference on human factors in computing systems*. 1–13.
- [89] 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 (2023), 1–35.
- [90] Sarah Prange, Pascal Knierim, Gabriel Knoll, Felix Dietz, Alexander De Luca, and Florian Alt. 2024. {“I”} do (not) need that {Feature!}—Understanding {Users’} Awareness and Control of Privacy Permissions on Android Smartphones. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. 453–472.
- [91] Sarah Radway, Katherine Quintanilla, Cordelia Ludden, and Daniel Votipka. 2024. An Investigation of US Universities’ Implementation of FERPA Student Directory Policies and Student Privacy Preferences. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. 1–35.
- [92] Counterpoint Research. 2025. Global VR Market Declines 12% YoY in 2024; ‘AR+AI’ Smart Glasses to Take Centre Stage in 2025. <https://counterpointresearch.com/en/insights/global-xr-arvr-headsets-market-2025>. Online; accessed Nov 2025.
- [93] Franziska Roesner, Tadayoshi Kohno, and David Molnar. 2014. Security and privacy for augmented reality systems. *Commun. ACM* 57, 4 (2014), 88–96.
- [94] Samsung. 2024. Use Facial recognition security on a Galaxy phone or tablet. <https://www.samsung.com/us/support/answer/ANS10002519/>. Online; accessed Nov 2024.
- [95] Samsung. 2024. Use the fingerprint sensor on your Galaxy phone or tablet. <https://www.samsung.com/us/support/answer/ANS10001613/>. Online; accessed Nov 2024.
- [96] Abhinaya SB, Abhisri Agrawal, Yaxing Yao, Yixin Zou, and Anupam Das. 2025. “What are they gonna do with my data?”: Privacy Expectations, Concerns, and Behaviors in Virtual Reality. *Proceedings on Privacy Enhancing Technologies* 2025, 1 (2025), 58–77.
- [97] Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. 2015. A design space for effective privacy notices. In *Eleventh symposium on usable privacy and security (SOUPS 2015)*. 1–17.
- [98] Alexis D Souchet, Domitile Lourdeaux, Jean-Marie Burkhardt, and Peter A Hancock. 2023. Design guidelines for limiting and eliminating virtual reality-induced symptoms and effects at work: a comprehensive, factor-oriented review. *Frontiers in psychology* 14 (2023), 1161932.
- [99] Statista. 2022. Sales of virtual reality head-mounted displays worldwide in 2016 and 2020. <https://www.statista.com/statistics/697159/head-mounted-display-unit-sales-worldwide/>. Online; accessed May 2025.
- [100] Meta Store. 2024. Meta Quest Tech Specs. <https://www.meta.com/quest/quest-pro-tech-specs/?srsltid=>

AfmBOoqWvjDL31r6GrDTz2nZ8T5ys1wxh1mKLnXfj18N4VPmnO-jBj.
Online; accessed Nov 2024.

- [101] Luma Tabbaa, Ryan Searle, Saber Mirzaee Bafti, Md Moinul Hossain, Jitrapol Intarasisrisawat, Maxine Glancy, and Chee Siang Ang. 2021. Vreed: Virtual reality emotion recognition dataset using eye tracking & physiological measures. *Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies* 5, 4 (2021), 1–20.
- [102] Junwei Tang, Ruixuan Li, Hongmu Han, Heng Zhang, and Xiwu Gu. 2017. Detecting permission over-claim of android applications with static and semantic analysis approach. In *2017 IEEE Trustcom/BigDataSE/ICSS*. IEEE, 706–713.
- [103] Eran Toch, Justin Cranshaw, Paul Hanks Drielsma, Janice Y Tsai, Patrick Gage Kelley, James Springfield, Lorrie Cranor, Jason Hong, and Norman Sadeh. 2010. Empirical models of privacy in location sharing. In *Proceedings of the 12th ACM international conference on Ubiquitous computing*. 129–138.
- [104] Tomislav Bezmalinovic. 2023. Quest 2 beats Quest 3 in sales, but what does that mean for the platform? <https://mixed-news.com/en/quest-2-vs-quest-3-amazon-sales-figures/>. Online; accessed Nov 2024.
- [105] Rahmadi Trimananda, Hieu Le, Hao Cui, Janice Tran Ho, Anastasia Shuba, and Athina Markopoulou. 2022. {OVRseen}: Auditing network traffic and privacy policies in oculus {VR}. In *31st USENIX security symposium (USENIX security 22)*. 3789–3806.
- [106] Güliz Seray Tuncay, Soteris Demetriou, Karan Ganju, and Carl A Gunter. 2018. Resolving the Predicament of Android Custom Permissions.. In *NDSS*.
- [107] 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.
- [108] Timothy Vidas, Nicolas Christin, and Lorrie Cranor. 2011. Curbing android permission creep. In *Proceedings of the Web*, Vol. 2.
- [109] Daniel Votipka, Seth M Rabin, Kristopher Micinski, Thomas Gilray, Michelle L Mazurek, and Jeffrey S Foster. 2018. User comfort with android background resource accesses in different contexts. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 235–250.
- [110] Jialin Wang, Rongkai Shi, Wenxuan Zheng, Weijie Xie, Dominic Kao, and Hai-Ning Liang. 2023. Effect of frame rate on user experience, performance, and simulator sickness in virtual reality. *IEEE Transactions on Visualization and Computer Graphics* 29, 5 (2023), 2478–2488.
- [111] Sinan Wang, Yibo Wang, Xian Zhan, Ying Wang, Yepang Liu, Xiapu Luo, and Shing-Chi Cheung. 2022. Aper: evolution-aware runtime permission misuse detection for Android apps. In *Proceedings of the 44th International Conference on Software Engineering*. 125–137.
- [112] Benjamin Watson, Victoria Spaulding, Neff Walker, and William Ribarsky. 1997. Evaluation of the effects of frame time variation on VR task performance. In *Proceedings of IEEE 1997 Annual International Symposium on Virtual Reality*. IEEE, 38–44.
- [113] Xuetao Wei, Lorenzo Gomez, Iulian Neamtii, and Michalis Faloutsos. 2012. Permission evolution in the android ecosystem. In *Proceedings of the 28th Annual Computer Security Applications Conference*. 31–40.
- [114] Primal Wijesekera, Arjun Baokar, Ashkan Hosseini, Serge Egelman, David Wagner, and Konstantin Beznosov. 2015. Android permissions remystified: A field study on contextual integrity. In *24th USENIX Security Symposium (USENIX Security 15)*. 499–514.
- [115] Primal Wijesekera, Arjun Baokar, Lynn Tsai, Joel Reardon, Serge Egelman, David Wagner, and Konstantin Beznosov. 2017. The feasibility of dynamically granted permissions: Aligning mobile privacy with user preferences. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1077–1093.
- [116] Primal Wijesekera, Joel Reardon, Irwin Reyes, Lynn Tsai, Jung-Wei Chen, Nathan Good, David Wagner, Konstantin Beznosov, and Serge Egelman. 2018. Contextualizing privacy decisions for better prediction (and protection). In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–13.
- [117] Andy Wai Kan Yeung, Anela Tosevska, Elisabeth Klager, Fabian Eibensteiner, Daniel Laxar, Jivko Stoyanov, Marija Glisic, Sebastian Zeiner, Stefan Tino Kulnik, Rik Crutzen, et al. 2021. Virtual and augmented reality applications in medicine: analysis of the scientific literature. *Journal of medical internet research* 23, 2 (2021), e25499.
- [118] Yuxia Zhan, Yan Meng, Lu Zhou, Yichang Xiong, Xiaokuan Zhang, Lichuan Ma, Guoxing Chen, Qingqi Pei, and Haojin Zhu. 2024. VPPet: Vetting Privacy Policies of Virtual Reality Apps. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security*. 1746–1760.

Acknowledgments

This work was supported by NSF Award 2440353, an NSF Graduate Research Fellowship Program Award, as well as gifts from Cisco and Google. The authors used generative AI-based tools to correct grammatical errors and awkward phrasing.

A Participant Demographics

B Interview Questions

PARTICIPANT'S VR BACKGROUND:

- (1) Can you give us a brief overview of your experiences with virtual reality?
- (2) Have you ever used it before?
- (3) How often (once, regularly, etc.)?
 - (a) If not, have you seen it be used?
- (4) What type of headset?
- (5) Where have you seen VR being used?
- (6) Have you ever used a headset before?
 - (a) What kind?
 - (b) In what context?
 - (c) How often?
- (7) What types of apps did you use?
- (8) Was it your device/someone else's?

PERMISSIONS UNDERSTANDING:

Questions are repeated for each app. Participants were asked about the three app groups (in brackets) in random order, but the order within each app group was consistent. [Beatsaber] [Youtube VR, Arkio] [Move Fast, Plank]

- (9) What types of data/data types do you think is being collected by this app?
- (10) How did you think this data was collected?
- (11) Why do you think that/how do you know?
- (12) Why do you think this data is being collected?
- (13) How do you think this data could be used?

VOICE:

Show participant the pop-up they saw in the YouTube VR app.

- (14) Was there anything about the warning that stood out to you?
- (15) What did you think it was requesting?
- (16) After giving the app access to the microphone, how long do you think it can record your microphone?
 - (a) Why do you think that?
- (17) Were there any other apps besides Youtube VR that you used that you think could record your microphone? Arkio? Plank or Move Fast?
 - (a) (If yes): Why do you think that?
 - (b) For how long?
 - (c) Under what conditions?

HAND-TRACKING:

Show participant the screen they saw when opening the Move Fast app, which prompts them to turn on hand tracking in settings.

- (18) Was there anything about the warning that stood out to you?
- (19) What did you think it was requesting?
- (20) How do you think hand tracking works? If you had to guess, how do you think it was tracking your hand?
- (21) After giving access to hand tracking, how long do you think it can track your hands? Why?
- (22) Do you think this impacts other apps' ability to use hand tracking?
 - (a) Why do you think that?
 - (b) (If yes): for how long? Under what conditions?

Participant Demographics				
Age	Gender	Race & Ethnicity	Education	Privacy Concern
18-23 (95.7%)	Man (73.9%)	White (39.1%)	H.S. or Below (30.4%)	Average 5.87
24-29 (4.3%)	Woman (26.1%)	African American (17.4%)	Some college (47.8%)	IUIPC Score:
30-39 (0%)	Non-Binary (0%)	Asian (34.8%)	Associate's (0%)	(Scale 1-7)
40+ (0%)		2 Or More Races (4.3%)	Bachelor's (17.4%)	VR Experience
		Other (4.3%)	or Above	30+ min (17.4%)
		Hispanic (13%),		<30 min (82.6%)
		Not Hispanic (87%)		

Table 1: Participant demographic information

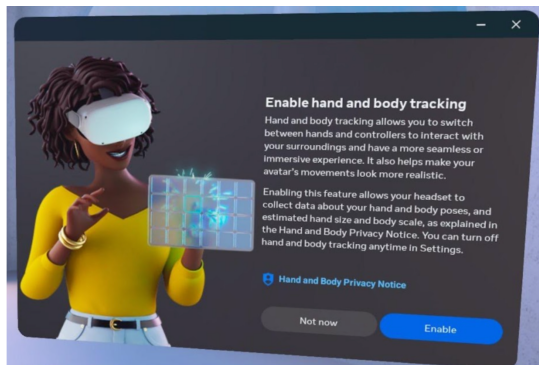


Figure 5: The first visual from the permission flow for hand tracking.

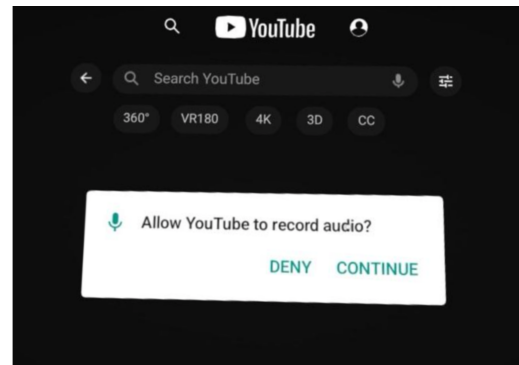


Figure 6: The microphone permission request seen by participants in Youtube VR.

Explain to the participant that the hand tracking permission request turned on hand tracking across all apps.

- (23) Why do you think this permission request takes place once?
- (24) Are you comfortable with the permission request taking place once?
- (25) Do you think the same policies should apply for hand tracking as for using a mouse?
- (26) Should Meta treat hand tracking data differently than mouse tracking data?
- (27) Do you see any differences between using the mouse, or the controllers, or your hands?
- (28) Do you see any differences between using the mouse, or the controllers, or your hands *for privacy*?
- (29) Do you view the data types collected by these modalities as the same?
- (30) Would you consider turning hand tracking off? For privacy reasons?

Explain biometric data collection to participant, including that data can be used to infer sensitive attributes, including identifying people, and diagnosing Parkinson's or ADHD.

- (31) Does this change your opinion about the permissions system?

C Permissions Flow