Identifying New Challenges In The Oculus Permissions Framework

Sarah Radway
Tufts University

Dan Votipka
Tufts University

1 Introduction

Virtual Reality (VR) is an emerging technology; with new technologies come new privacy threats. VR requires fine-grained collection and use of sensitive biometric data. While other previous works have examined privacy leakage from VR data (such as identity and personal attributes) [2,4,5], in this work, we begin to examine how the permissions framework surrounding data use and collection in VR compares with existing technology—namely, with the current Android model. Through doing so, we may begin to understand how permissions models in existing systems are applied to VR.

2 RQ1: How is user data collection described in documentation?

In order to understand what data is important to protect, we wanted to understand what data is collected by VR devices, and for what purposes. Thus, for all documentation for Meta's Oculus Quest for Native development, as well as Unity and Unreal Engine (the two popular VR development platforms), we noted each function call and extension listed that required user data and listed the function call's use/application as described to the developer in the documentation. We grouped the calls into overarching categories based upon the data types they collected; these groups are shown in Table 1.

We see that VR's biometric tracking is necessary for various functionalities, and much more involved than with previous technologies; while a FitBit has an accelerometer to track general movements, tracking in VR is far more fine-grained.

Data Type	Documented Use
Eye Tracking	To “enhance social presence" & interact with the scene
Face Tracking	To ”enhance social presence”
Head Tracking	To update the FOV
Hand Tracking	To position game objects and detect hand poses
Body Tracking	To “bring a user's physical movements into the metaverse and enhance social experiences”
Surroundings	To “validate the user-defined boundary" and use “passthrough visualization"
Input	“To accurately detect the user's interaction”
Voice Input	To create “natural and flexible ways for people to interact with the app"
Device Info	To create warnings when, for example, “device temperature reaches the limit"
Location	To translate or specify information for different user locations
Network Info	To check network connection status
PII & Identifiers	Lets developers “easily understand game performance and player behaviors”

Table 1: The purposes for various types of data collection as listed in Oculus Quest, Unity, and Unreal documentation.

3 RQ2: What VR apps request access to different user data?

We then sought to understand how many apps requested permissions associated with data collection in VR. We downloaded the 107 free Oculus apps available in the Meta Quest Store. We extracted the manifests and collected the features and permissions in the manifests of each app, and organized them into the data type categories outlined in Section 2. We report the frequency at which different data types are requested in Table 2, with example permissions and features for each category. We see that VR's biometric tracking is much more

USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.
August 6–8, 2023, Anaheim, CA, USA

Data Type	Oculus (/107)	Android (/192)
Eye Tracking	11	0
Face Tracking	10	0
Head Tracking	105	0
Hand Tracking	36	0
Body Tracking	3	4
Surroundings	37	117
Input	0	0
Voice Input	73	92
Device Info	98	192
Location	15	120
Network Info	98	192
PII & Identifiers	27	186

Table 2: The number of Android applications and Oculus applications requesting permissions from each of the categories.

involved than with previous technologies; while a FitBit may have an accelerometer to track general movements, tracking in VR is much more fine-grained. Documentation suggests that VR's collection and processing of users' biometric data is necessary for various functionalities.

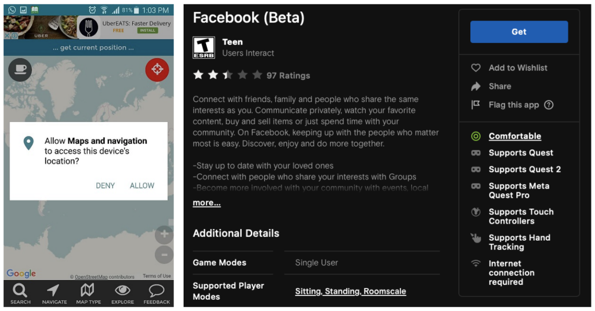
4 RQ3: How is this different from existing technology?

Next, we sought to understand how the results compare with existing permissions systems–namely, with Android phones. We downloaded the Top 200 free Android applications available in the Google Play Store. As in Section 3, we collected the features and permissions in the manifests of each app, and sorted them into the data type categories shown in Table 2.

We see that the data of concern is very different: Android devices collect much more information about users' location and network; permissions in Oculus are much more centered around biometric information, such as eye, face, head, hand, and body tracking, as well as the microphone.

5 RQ4: How are users being informed of data use and collection?

For Android applications, many sensitive permissions are run-time permissions: the system presents a permission prompt upon download or "before each access" [1]. For Oculus, permissions present in old Android applications work more or less the same way. However, the new permissions required for VR (i.e. eye, face, hand tracking) were requested once for all apps (i.e. the first time any app requests it), and then become install-time permissions. This means that they are displayed on the App Store page, as shown in Figure 1, and automatically granted at install time.


1:03 PM
81%
UberEATS: Faster Delivery
FREE
INSTALL
UBER
... get current position ...
Google
© OpenStreetMap contributors
Terms of Use
SEARCH
NAVIGATE
MAP TYPE
EXPLORE
FEEDBACK

Allow **Maps and navigation** to access this device's location?

DENY ALLOW

Facebook (Beta)

Teen
Users Interact

97 Ratings

Connect with friends, family and people who share the same interests as you. Communicate privately, watch your favorite content, buy and sell items or just spend time with your community. On Facebook, keeping up with the people who matter most is easy. Discover, enjoy and do more together.

-Stay up to date with your loved ones
-Connect with people who share your interests with Groups
-Become more involved with your community with events, local

more...

Additional Details

Game Modes	Single User
Supported Player Modes	Sitting, Standing, Roomscale

Figure 1: An Android run-time permission on the left, and an Oculus install-time permission on the right.

6 Discussion

Our study demonstrates that VR requires the collection of biometric data for functionality at a far greater frequency and depth than previous devices. In comparison with Android phones, VR devices collect much less information regarding users' locations and network information, and far greater information about the user's body and voice.

We must consider how the data collected in VR, and its potential uses, ought to drive the permissions framework. In Android, 'dangerous' permissions are flagged at runtime [1]; Oculus, alternatively, doesn't use a purely run-time permissions system, but often relies upon an hybrid approach for biometric data. This approach of implicit authorization makes sense 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. However, it is worth considering whether this approach could introduce bad mental models of the app's behavior and data collection practices, as Micinski et al. explored in the context of the Android permissions system [3]. If notice and consent is the appropriate framework, this implementation could be improved to allow users greater understanding of data use. However, it is unclear whether notice and consent is the right framework for the privacy concerns associated with VR; given the sensitive uses of biometric data, regulation surrounding data **use** may be necessary.

7 Future Work

Moving forward, we plan to expand beyond the limited applications evaluated in this initial investigation. We will also begin looking at the code run on Oculus devices; using our list of compiled function calls, we can use a tool like Androguard to understand when functions are being called, and thus when data is being collected. We are also performing a user study looking at how users form mental models in the VR setting.

References

[1] Permissions on Android (https://developer.android.com/guide/topics/permissions/overview).

[2] Jaybie A de Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. A first look into privacy leakage in 3d mixed reality data. In *Computer Security–ESORICS 2019: 24th European Symposium on Research in Computer Security, Luxembourg, September 23–27, 2019, Proceedings, Part I 24*, pages 149–169. Springer, 2019.

[3] Kristopher Micinski, Daniel Votipka, Rock Stevens, Nikolaos Kofinas, Michelle L Mazurek, and Jeffrey S Foster. User interactions and permission use on android. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 362–373, 2017.

[4] Mark Roman Miller, Fernanda Herrera, Hanseul Jun, James A Landay, and Jeremy N Bailenson. Personal identifiability of user tracking data during observation of 360-degree vr video. *Scientific Reports*, 10(1):1–10, 2020.

[5] Vivek Nair, Gonzalo Munilla Garrido, and Dawn Song. Exploring the unprecedented privacy risks of the metaverse. *arXiv preprint arXiv:2207.13176*, 2022.