Identifying New Privacy Challenges In The Oculus Permissions Framework

Sarah Radway, Dan Votipka (Tufts University)

Abstract

- 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).
- 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.

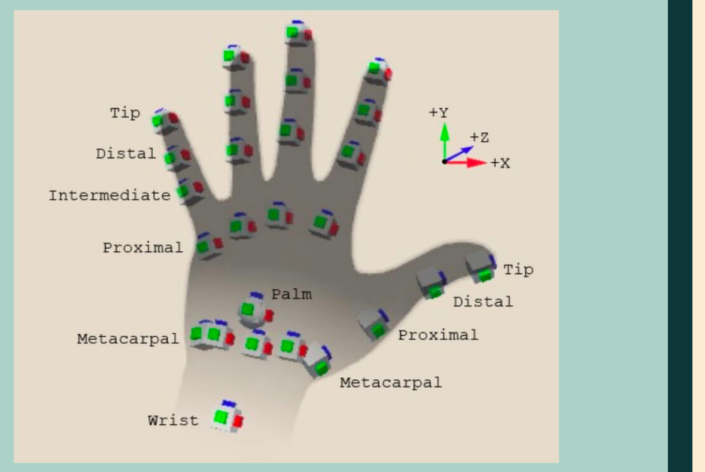
RQ1: How is user data collection described in documentation?

Methodology: 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. We grouped the calls into categories based upon the data types they collect, and listed their uses as described to the developer in the documentation:

Data Type	Documented Use
Eye Tracking	• "[Allows] a user's character representation to make eye contact with other users, significantly improving social presence" • "Can be used...in order to select objects in a scene" • "To render full resolution where you are looking at...and low pixel density in the periphery"
Face Tracking	• "Allows developers to use abstracted facial expression data to enhance social presence" • "Face tracking can help make a character's facial expression look more natural during virtual interactions with other users"
Head Tracking	• "Required for v2 signing, which is required for store review for Meta Quest apps" • Necessary to update FOV
Hand Tracking	• "Let you render a skinned hand mesh, use collision capsules, and a ray-cast-plus-pinch UI interaction model" • "To position game objects or other visual representations of the hands" • "To detect hand poses"
Body Tracking	• "To bring a user's physical movements into the metaverse and enhance social experiences."
Surroundings	• "The guardian system validates the user-defined boundary for the minimum required space." • "Allows developers to integrate the passthrough visualization with their virtual experiences." • "Lets users walk around and capture their scene to generate a Scene Model"
Input	• "To accurately detect the user's interaction with the controller and enable a variety of control schemes"
Voice Input	• "To enhance the AR/VR experience with more natural and flexible ways for people to interact with the app. For example, voice commands can shortcut controller actions with a single phrase, or interactive conversation"
Device Info	• "The device temperature reaches the limit...Apps may choose to continue operating in a degraded fashion, perhaps by changing to 30 FPS. Others may display a warning screen saying that play cannot continue."
Location	• "Localization gatherer takes care of capturing the text so that it can be localized [i.e. translated]"
Network Info	• To check network connection status
PII & Identifiers	• "Lets studios easily understand game performance and player behaviors"

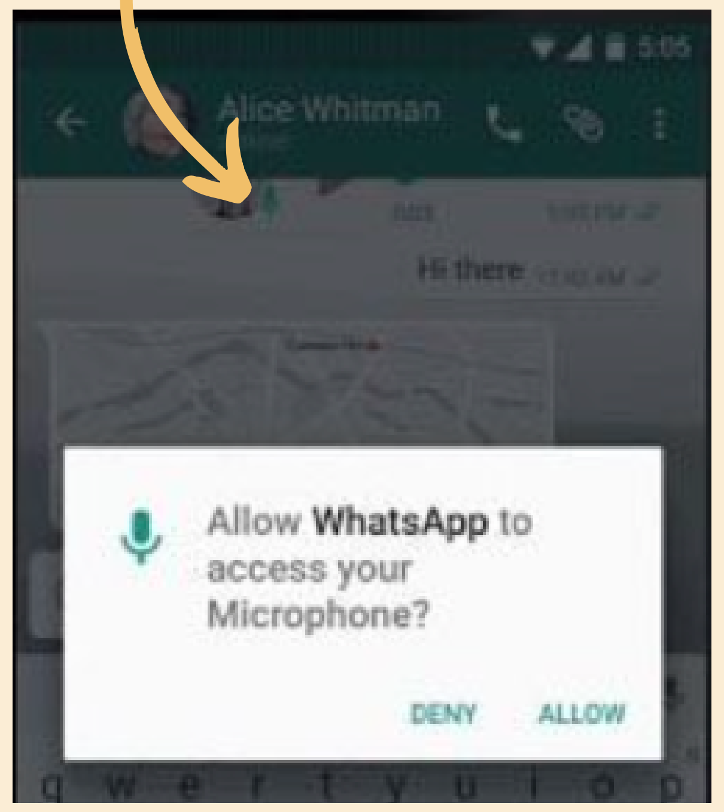
- **VR's biometric tracking is much more involved than with previous technologies; while a FitBit may have an accelerometer to track general movements, tracking in VR is much more fine-grained.**
- **VR's collection and processing of users' biometric data is necessary for various functionalities.**

i.e. a model of the tracked points on a user's hand from Unity docs



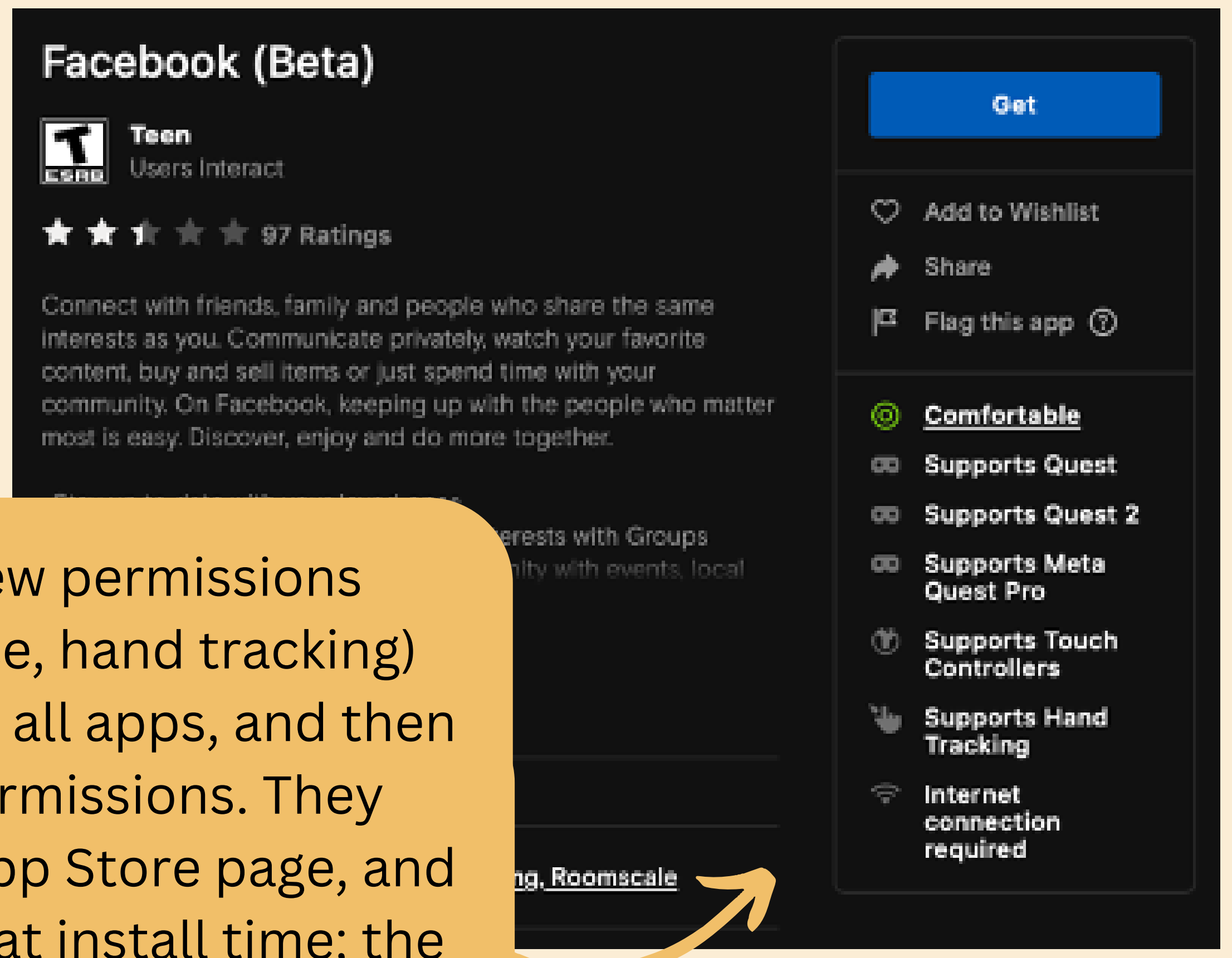
RQ4: How are users being informed of data use and collection?

For Android, many of the sensitive permissions are runtime permissions. This means that they are requested at run time. Less sensitive permissions are shown in the app store (at install-time).



Allow **WhatsApp** to access your Microphone?

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.

...erests with Groups
...nity with events, local

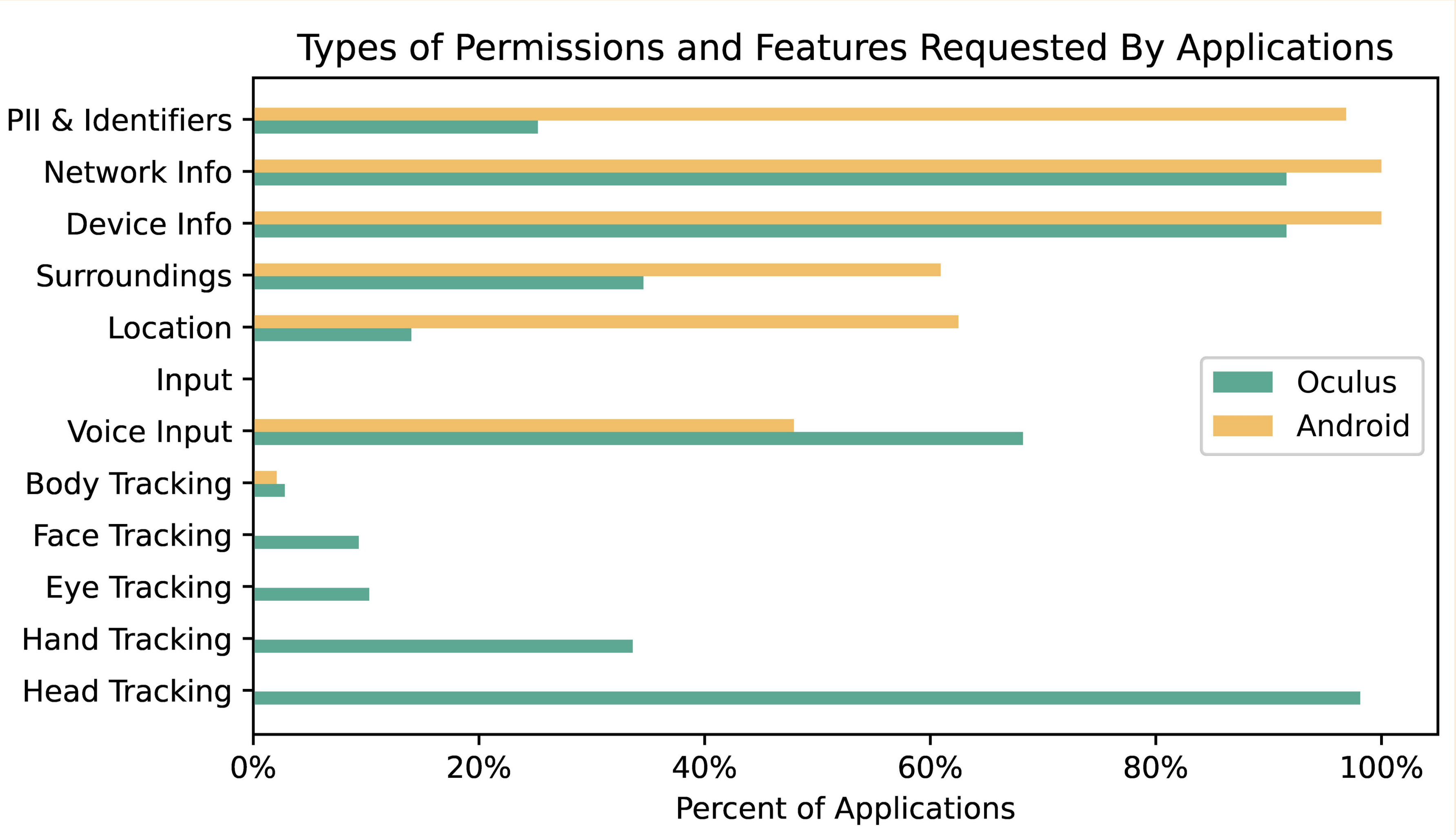
...ng, Roomscale

Comfortable
Supports Quest
Supports Quest 2
Supports Meta Quest Pro
Supports Touch Controllers
Supports Hand Tracking
Internet connection required

For Oculus, it seems new permissions required for VR (i.e. face, hand tracking) are requested once for all apps, and then become install time permissions. They are displayed on the App Store page, and automatically granted at install time; the user does not acknowledge them on a per-app basis.

RQ2: What VR applications request access to different user data?

Methodology: We downloaded the 107 free Oculus applications available in the Meta Quest Store, and collected the features and permissions in the manifests of each app. We organized each of these collected requests into data type categories.



RQ3: How is this different from existing technology?

Methodology: We downloaded the Top 192 free Android applications available in the Google Play Store, and analyzed the Manifests in the same way as in RQ2.

Limitation: In this initial study, we only evaluate a limited range of applications. We will expand this to include more applications in future work.

- **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 voice input. The data of concern is very different.**
- **Notably, VR applications requests permission to record voice data/access the microphone more frequently than Android applications.**

Takeaways

1. 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.
2. As Oculus develops a new framework for permissions surrounding sensitive biometric data, we must consider how the data collected in VR, and its potential uses, ought to drive the permissions framework. It is unclear whether notice and choice is a sufficient framework; given the sensitive uses of biometric data, regulation surrounding data use may be necessary.

Future Work

- Expand beyond the limited applications evaluated in this initial investigation. We are also performing a user study looking at how users form mental models in the VR setting.
- We plan to 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.
- Consider how we can modify existing privacy models moving forward for VR devices.