OVRSeen

Auditing Network Traffic and Privacy Policies in Oculus VR

R. Trimananda, H. Le, H. Cui, J. T. Ho, A. Shuba, A. Markopoulou

UCI ProperData

SCAN ME

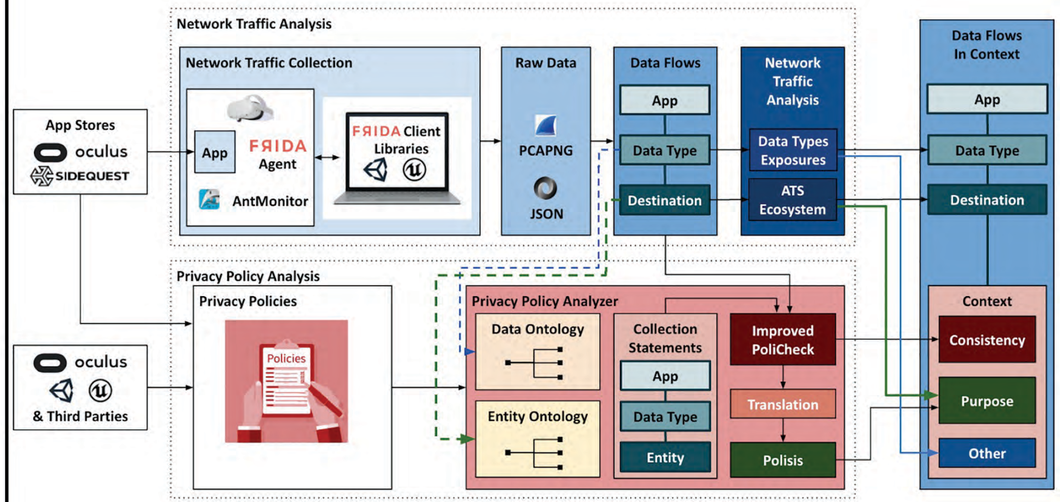
Motivation

- Virtual reality (VR) devices, such as the Oculus VR (OVR), introduce privacy risks unique to the platform because, unlike other platforms and devices, they are equipped with many sensors that may collect user's biometric data.

Contributions

- Large-scale measurement and characterization of privacy aspects of 140 OVR (free and paid) apps from a combined network traffic and privacy policy perspective.
- Decrypt network traffic on Oculus VR, using static and dynamic analysis.
- Improve on state-of-the-art NLP tools for privacy policy analysis to check the consistency between network traffic and privacy policy based on the Contextual Integrity (CI) framework.

System Overview



Broader Impact

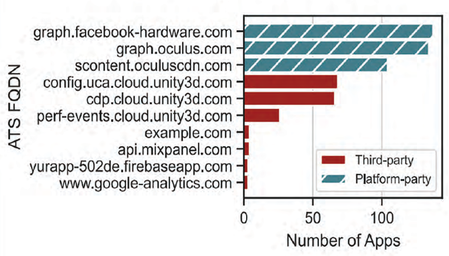
FTC PrivacyCon 2022: Our team was invited to present OVRseen at FTC PrivacyCon 2022.

Other Events: OVRseen was also presented at PrivaCI Symposium 2022, and a DuckDuckGo corporate event.

Responsible Disclosures: We contacted the developers of the 140 apps about our findings. They appreciated this and expressed their willingness to adopt our recommendations to improve their privacy policies.

Network Traffic Analysis

Top-10 Ads/Tracking Destinations

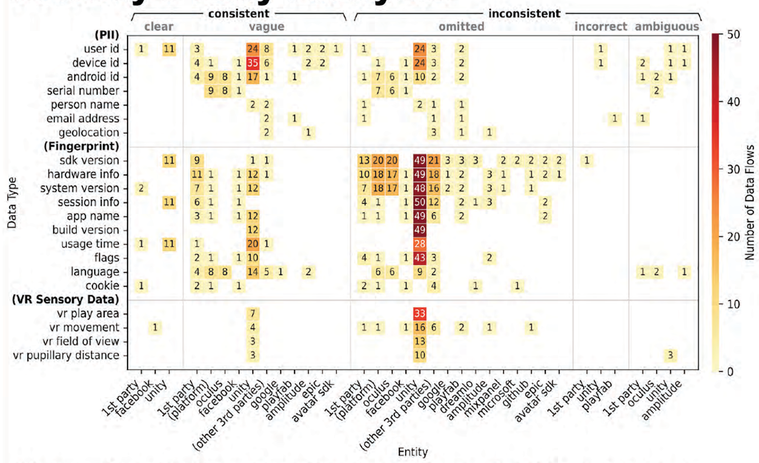


Data Types Exposed

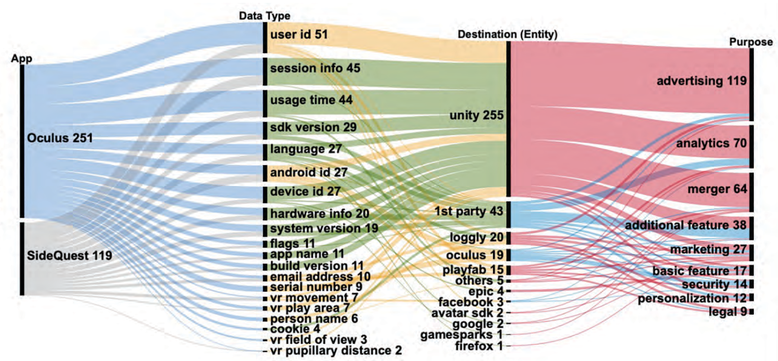
Data Types (21) / PII	Apps 1st	Apps 3rd	Apps Pl.	FQDNs 1st	FQDNs 3rd	FQDNs Pl.	% Blocked 1st	% Blocked 3rd	% Blocked Pl.
Device ID	6	64	2	6	13	1	0	38	100
User ID	5	65	0	5	13	0	20	38	-
Android ID	6	31	18	6	7	2	17	43	50
Serial Number	0	0	18	0	0	2	-	-	50
Person Name	1	7	0	1	4	0	0	50	-
Email	2	5	0	2	5	0	0	20	-
Geolocation	0	5	0	0	4	0	-	50	-
VR Sensory Data									
VR Play Area	0	40	0	0	1	0	-	100	-
VR Movement	1	24	2	1	6	1	0	67	100
VR Field of View	0	16	0	0	1	0	-	100	-
VR Pupillary Distance	0	16	0	0	1	0	-	100	-

Summary: The advertising and tracking ecosystem of Oculus VR is still developing: most traffic went to Oculus, Facebook, and Unity. No ad-requests were found as there are no on-device ads. We found 21 data types, for which state-of-the-art blocklists only captured 36% of exposures to third parties, missing some sensitive data types such as Email, User ID, and Device ID.

Privacy Policy Analysis



Network-to-Policy Consistency: Around 70% of data flows from OVR apps were inconsistent with the collection statements in the privacy policies: these privacy policies did not reference privacy policies from third parties (e.g., Unity).



Data Flows in Context: 69% of data flows were associated with purposes unrelated to the core functionality (e.g., advertising, marketing, analytics).