Privacy of Virtual Reality: Our Future in the Metaverse and Beyond

commonsense.org/privacy-of-virtual-reality

common sense®

"There has been an increasing focus only on the benefits of VR, with very little research on the costs to users' privacy."

Key Findings and Takeaways

1. Not a single VR headset that we reviewed has earned our recommendation for kids, meaning that every single device in one way or another puts kids' personal privacy or safety at serious risk.
2. Every tested device is exploiting users' data for profit, and the collected data is more sensitive and intimate than other media, including body posture, eye gaze, pupil dilation, gestures, facial expression, and even minute variations in skin color.
3. There are some ways to make VR devices safer if kids use them, including options to turn off some of the most problematic data collection, and turn on privacy and safety settings.
4. But settings put the burden on the parent, caregiver, or educator to keep kids safe, and navigate hard-to-find and complex privacy and safety options that are always changing.

Table 2: Privacy rating criteria of virtual reality devices

Product	Privacy Rating	Sell Data	Third-Party Marketing	Targeted Ads	Third-Party Tracking	Track Users	Ad Profile
Microsoft HoloLens 2[a]	75% Warning	No	Yes	Yes	Yes	Yes	Yes
HP Reverb G2[b]	63% Warning	No	Yes	Yes	Yes	Yes	Yes
HTC Cosmos Elite[c]	63% Warning	Yes	Yes	Yes	Yes	Yes	Yes
PlayStation VR[d]	59% Warning	No	Yes	Yes	Yes	Yes	Unclear
Meta Quest 2[e]	55% Warning	No	Yes	Yes	Yes	Yes	Yes
Valve Index[f]	50% Warning	Unclear	Unclear	Unclear	Unclear	Unclear	Unclear
Pimax Vision 5K[g]	30% Warning	Unclear	Yes	Yes	Unclear	Unclear	Unclear

[a] *See* Common Sense Privacy Evaluation for Microsoft HoloLens, https://privacy.commonsense.org/evaluation/Microsoft-Hololens.
[b] *See* Common Sense Privacy Evaluation for HP Reverb G2, https://privacy.commonsense.org/evaluation/HP-Reverb-G2.
[c] *See* Common Sense Privacy Evaluation for HTC Vive, https://privacy.commonsense.org/evaluation/HTC-Vive.
[d] *See* Common Sense Privacy Evaluation for PlayStation, https://privacy.commonsense.org/evaluation/PlayStation.
[e] *See* Common Sense Privacy Evaluation for Oculus, https://privacy.commonsense.org/evaluation/Oculus.
[f] *See* Common Sense Privacy Evaluation for Valve Index, https://privacy.commonsense.org/evaluation/Valve-Index.
[g] *See* Common Sense Privacy Evaluation for Pimax, https://privacy.commonsense.org/evaluation/Pimax.

This is a critical moment

This is a critical moment in our history to demand better privacy practices from VR companies and put in place stronger privacy regulations of VR technologies to help reshape what privacy in virtual reality and the metaverse means for all of us.

- At this moment, we have a rare chance to think about and implement appropriate privacy and safety design policies.
- We can create best practices for the use of sensitive information before VR is fully adopted and integrated into society.
- We need to ensure safe education and play spaces for children in VR, because many users experience sexism, racism, homophobia, and other forms of harassment, stalking, and abuse. It is critical that these platforms, the content, and experiences they provide are age appropriate and privacy protective.
- This is also a chance for us to define what “privacy” means in VR before it becomes too late to look at what should have been considered and adopted from the beginning.

We can’t recommend VR headsets

Not a single VR headset we tested in the market right now has earned our recommendation for kids or teens.

- All seven of the most popular devices we looked at do not meet our minimum requirements for privacy and security practices. Here's what we found:
    - Users are tracked from the moment they put on any of these VR devices.
    - Privacy policies were unclear or said sensitive data is used for targeted advertising, third-party marketing, and tracking purposes.
    - None of these devices use privacy-by-design.
    - They all displayed third-party advertising to users.
- Not only are there none of these baseline protections, they also lack specific protections for kids under 13 who use these devices.
    - For example, more than half (57%) of the devices have no parental controls, and less than a third(1/3) had any safety settings at all.

Data Collection for Profit

The bottom line is that every VR device we tested exploits users' sensitive data collected in virtual reality for profit.

- VR devices collect much more data than mobile apps and websites—including body posture, eye gaze, pupil dilation, gestures, and facial expression – even as specific as minute variations in skin color
    - A user's body movements in VR are tracked more than 100 times per second, which means spending 30 minutes or more in a VR simulation can collect over 2 million unique data points.
- In many cases, these automatic body responses and functions can betray our innermost thoughts and feelings that we may feel are private because users not only see VR, but they experience it.
- Researchers have demonstrated that media-rich VR environments can create unique opportunities to influence users' behavior, encourage riskier choices, increase prolonged use, and even implant false memories.
- All of this emphasizes why change needs to happen now – before these opportunities become reality.

Safer Privacy Settings

All that said, there are ways to make some devices safer if kids want to use them – or already own them.

- Many of the devices we reviewed – some that are the most popular with kids – do have options to turn off or on some of the most problematic data collection and safety settings.
- But that puts the burden on the parent or caregiver or educator to keep kids safe, and navigate hard to find and complex privacy and safety options.
- But if your child uses one of these devices, it's extremely important for parents/caregivers to use the few options they have to limit data collection and protect privacy.
- Teens and students older than 13 should only use virtual reality devices and applications when an adult is present to supervise and limit use while following age-appropriate screen-time recommendations.

The Industry Can Change

The industry can take steps today to ensure kids can experience what these technologies can offer – but safely.

- There should be more privacy settings for VR devices and applications to restrict sensitive data collection and require data minimization for first-party and third-party applications.
- VR devices should include privacy settings that restrict advertising, marketing, and tracking purposes that also apply to and restrict third-party apps, not just the VR device and its first-party apps.
- Finally, companies need to be more transparent in their privacy policies about new types of data collected from VR, how they protect children's data, and the new types of biometric-derived advertising use that is potentially far more invasive and exploitative than any other form of targeted advertising known to date.
- If we make our voices heard – tell companies we want safer VR for our kids – we can make meaningful change happen.

Contact us

The report and executive summary are available below. Please contact us with any questions or comments.

commonsense.org/privacy-of-virtual-reality

gkelly@commonsense.org

Thank you