PRIVACY LAW

CALIFORNIA LAWYERS ASSOCIATION

presents

Inaugural Annual Privacy Summit

Session 7, Track 2

The Future is the Metaverse, but Privacy Risks are Now!

MCLE: 1.0 Hours

Friday, February 10, 2023
2:00 p.m. – 3:00 p.m.

Speakers:

Emily Yu, Senior Director of Product Counsel, Roblox
Jill Bronfman, Privacy Counsel, Common Sense Media

Conference Reference Materials

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

common sense®

Credits

Authors:	Girard Kelly, Common Sense Media Jeff Graham, Common Sense Media Jill Bronfman, Common Sense Media Steve Garton, Common Sense Media
Contributors:	Olivia Figueira Aya Nouiouat
Data analysis:	Girard Kelly, Common Sense Media Jeff Graham, Common Sense Media
Copy editors:	Christopher Dare, Common Sense Media Jennifer Robb
Designer:	Jeff Graham, Common Sense Media
Photo:	iStock/boana

Suggested citation: Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2022). *Privacy of Virtual Reality: Our Future in the Metaverse and Beyond*. San Francisco, CA: Common Sense Media.

Table of Contents

Introduction

When superheroes gather to confer about saving the world, it's usually pretty clear not only whether they will prevail, but how. Each will use their well-known and well-tested superpowers to engage with the villains and battle for what we know is good and right in the world. However, to understand what justice means in the story, we need to know who we're dealing with in order to set things right. We need to understand who is the antagonist of our story, and to quickly stop whatever schemes they have in mind before time runs out and it's too late to save the world.

This report tells the story about an emerging technology used by kids and families every day, and the plot behind that technology to take over the world. But fortunately, it's not too late. This is a story about all of us, and we just so happen to be the protagonists in this particular time and place who are fighting for our fundamental human right to privacy. It's also a story about what privacy means for everyone at a pivotal moment in the history of humankind, when we have a unique opportunity to reflect and come together to decide the future of privacy of an emerging technology.

If this story sounds familiar, it's because you may have already heard it before. It has been popularized in books, games, and media culture, with recent movies for kids and teens like Ready Player One,[1] where our hero Wade (Parzival) declares an all-out virtual reality war on a profit-seeking corporation, called the Sixers, for control of the Oasis. In the real world, this plot sounds a lot like our collective fight for the right to privacy and control of the metaverse from profit-seeking corporations. Other popularized films, such as Ron's Gone Wrong,[2] are easily analogized to corporations selling us our must-have technology, including mobile devices, laptop computers, and virtual assistants. The Mitchells vs. the Machines[3] is the story of a family's fight against artificial intelligence robots that decide to take over the world for the benefit of a monopolistic social media company. In an effort to portray the ethical quagmire that is a virtual afterlife, the Black Mirror episode "San Junipero"[4] and the TV series Upload[5] explore who would and would not choose this mode of existence, as well as the commercial possibilities of such a virtual reality universe.

But these popularized media narratives are moving out of the realm of science fiction and into our shared experiences with virtual reality. At this very moment, the antagonists of our story are the same corporations selling us cutting-edge virtual reality devices and immersive virtual reality applications. This new immersive world has already been given a name—the metaverse—which is meant to describe all the present and future virtual reality devices and applications that users will experience and drive a new virtual creative economy.[6]

The promise is that the metaverse will be used for social good and that it will be the next era of computing, following the adoption of mainframes, personal computers, mobile devices, and the cloud. The impact of the metaverse is still unknown, except that it is intended to connect people with virtual reality devices to limitless 3D virtual experiences for the purposes of entertainment, gaming, education, collaboration, and communication.[7]

Virtual reality (VR) technology[8] exists most certainly in the present, rather than solely in the future or as the subject of science fiction movies, and it is already a

[1] *See Ready Player One* (2018): https://www.imdb.com/title/tt1677720.

[2] *See* Ron's Gone Wrong (2021): https://www.imdb.com/title/tt7504818.

[3] *See The Mitchells vs the Machines* (2021): https://www.imdb.com/title/tt7979580.

[4] For a synopsis, see https://black-mirror.fandom.com/wiki/San_Junipero.

[5] For episode synopses, see https://en.wikipedia.org/wiki/Upload_(TV_series).

[6] *See* The Metaverse and How We'll Build It Together – Connect 2021: https://www.youtube.com/watch?v=Uvufun6xer8.

[7] *See* Ball, M. (2022, July 18). The metaverse will reshape our lives. Let's make sure it's for the better. *Time*. https://time.com/magazine/south-pacific/6201603/august-8th-2022-vol-200-no-5-asia-europe-middle-east-and-africa-south-america-south-pacific.

[8] With virtual reality technology, wearing headsets in the real world allows people to interact almost seamlessly in the virtual world. While people are currently limited to using an avatar in VR, or part of one, the avatar is not wearing any sort of apparatus, and it appears to be "you." Similarly, augmented reality (AR) adds or supplements our existing reality with digital objects and digital object overlays in the real world. AR enhances our presence by augmenting reality, which while it still allows a user to stay in a real space and time, may collect personal information from users at an astonishing rate. Mixed or merged reality (MR) uses holographic lenses to converge VR and AR where virtual objects interact with real world objects and users can transition between completely immersive VR environments to augmented AR environments. Finally, extended reality (XR) is a catchall term to include all the different types of experiences in VR, AR, and/or MR.

multibillion-dollar industry.[9] The potential benefits[10] of virtual reality could transform different segments of society in countless positive ways,[11] similar to how personal computers and mobile devices have changed our everyday lives in ways that were unimaginable even just a few decades prior.[12] However, we need to make sure the potential harms of virtual reality do not outweigh their potential benefits—otherwise we risk transforming society into a dystopian future that science fiction[13] has tried to warn us about.

In the past, thoughts of privacy and the social, ethical, and legal effects of technology have typically only been considered after the fact. In this moment, we have a rare chance to think about and implement appropriate design policies and use of information restrictions and guidance before its greater adoption and integration into society. 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.

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

This report seeks to explore some of the potential risks and harms by determining the actual privacy practices as well as the potential developmental and psychological implications of popular virtual reality devices and third-party VR applications used by kids and families today, and how the data collected in virtual reality is used by companies for commercial purposes and profit.[14] Our findings indicate that all of the popular virtual reality devices we tested are not privacy protective and do not meet our privacy recommendations for use by kids and families.

When your superpower is data extraction

Virtual reality hardware and software enable superhuman data collection and distribution. VR hardware can collect human biometric[15] and sensory data, and the software gathers human experience and reactions,[16] far beyond what we have come to expect from simply typing our thoughts and feelings into a computer or mobile device. VR works as an extraction system to collect and process personal information in a way that no single human or portal could using previous technology.[17] This is a quantitative and possibly qualitatively larger undertaking to automatically collect more personal and behavioral information than any user could possibly input voluntarily.[18]

As VR technology becomes ubiquitous in public spaces, processing a bystander's data poses a separate privacy risk because that bystander may not have situational awareness that their facial recognition or other bodily information is being collected from potentially multiple VR devices. In addition, bystanders have no way of opting out of the collection or use of their personal information[19] by companies they do not know and have no

[9] *See* Alsop, T. (2022, August 11). Virtual reality (VR) – statistics & facts. *Statista*. https://www.statista.com/topics/2532/virtual-reality-vr.

[10] "There continue to be questions around the longevity and potential of the metaverse, with an extreme view regarding it as merely a rebranded gaming platform of little wider interest. We do not share that skepticism and believe the metaverse has the potential to be the next iteration of the internet." McKinsey & Company. (June 2022). *Value creation in the metaverse*. https://www.mckinsey.com/~/media/mckinsey/business%20functions/marketing%20and%20sales/our%20insights/value%20creation%20in%20the%20metaverse/Value-creation-in-the-metaverse.pdf.

[11] Jerome, J., & Greenberg, J. (April 2021). Augmented reality + virtual reality: Privacy & autonomy considerations in emerging, immersive digital worlds. The Future of Privacy Forum. https://fpf.org/wp-content/uploads/2021/04/FPF-ARVR-Report-4.16.21-Digital.pdf.

[12] *See* Aubrey, J. S., Robb, M. B., Bailey, J., & Bailenson, J. (2018). Virtual reality 101: What you need to know about kids and VR. *Common Sense Media*. https://www.commonsensemedia.org/sites/default/files/research/report/csm_vr101_final_under5mb.pdf; *See also* Bailey, J.O., & Bailenson, J. (2017). Considering virtual reality in children's lives. *Journal of Children and Media*, 11:1, 107–113. https://stanfordvr.com/mm/2017/02/bailey-jcm-considering-vr.pdf; Heller, B. Carr Center for Human Rights Policy, Reimagining Reality: Human Rights and Immersive Technology, https://carrcenter.hks.harvard.edu/files/cchr/files/ccdp_2020-008_brittanheller.pdf.

[13] Margaret Atwood, the author of The Handmaid's Tale, has been photographed with a mug saying "I Told You So" (see https://happymag.tv/margaret-atwoods-i-told-you-so-mug-is-proving-to-be-divisive/) in reference to her dystopian novel where, among other surveillance issues, pregnancy and fertility are managed by the state. For current and future data collection and sale potential, including a discussion of policy, see, e.g., https://gizmodo.com/data-brokers-selling-pregnancy-roe-v-wade-abortion-1849148426.

[14] "Expenditure on these technologies in the global education market is expected to grow from $1.8 billion in 2018 to $12.6 billion in 2025, at a CAGR of 32%." The Metaverse in Education - Market Size & Activity, EdtechX Email Newsletter, May 5, 2022.

[15] "Biometric information" means an individual's physiological, biological, or behavioral characteristics that are used to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, as well as keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, and exercise data that contain identifying information. *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.40(c).

[16] *See* list of possible data collection in Zhao, et. al, "VR in Metaverse: Security and Privacy Concerns," available at https://arxiv.org/pdf/2203.03854.pdf.

[17] "Many apps still collect device information that can be used to track users at a group level (cohort tracking) or identify individuals probabilistically (fingerprinting). We find real-world evidence of apps computing and agreeing on a fingerprinting-derived identifier through the use of server-side code." Kollnig, K., Shuba, A., Kleek, M.V., Binns, R., & Shadbolt, N. (2022, May 7). Goodbye tracking? Impact of iOS app tracking transparency and privacy labels. https://arxiv.org/pdf/2204.03556.pdf.

[18] *See*, for example, media coverage of data collection potential and possibilities, even with early versions of the devices, in 2018 at https://www.windowscentral.com/vr-and-your-privacy-how-are-these-companies-treating-your-data, and in 2019 at https://hellodarwin.com/blog/virtual-reality-data-collection.

[19] Pahi, S., & Schroeder, C. *Extended privacy for extended reality: XR technology has 99 problems and privacy is several of them.* https://ssrn.com/abstract=4202913.

relationship with. Furthermore, VR devices may blur the line between public and private spaces, where through use of visual and auditory sensors, private spaces (such as bedrooms) can unexpectedly become public.[20]

However, we do not need to accept that our raw private experiences, feelings, and emotions[21] in virtual reality are the sole property of corporations. We do not need to accept that virtual reality device manufacturers and third-party application developers are allowed to capture our collective experiences in virtual reality as behavioral data to be used for commercial purposes and profit.[22] We can reject the premise that virtual reality is simply a means to an end for companies to engage in amplified data collection, behavioral manipulation, and commercial exploitation for their benefit, not ours. Perhaps our fundamental human right to privacy does override the "rights" of technological innovation driven by surveillance capitalism.[23] This is a critical moment in our history to demand better privacy practices from companies and put in place stronger privacy regulations of VR to help reshape what privacy in virtual reality and the metaverse means for all of us.

We need to examine what types of personal information and uses of data should be off-limits. If we illuminate the current status of VR privacy, we have a unique opportunity to create parameters for privacy protection in law for this largely unregulated sphere. We can consider the risks and harms to children and other vulnerable users, and craft standards to meet their needs.[24] These standards can be baked into future VR devices and applications as a matter of privacy by design, industry standards, and regulatory requirements.

Corporate ownership: To metaverse and beyond

Unlike the birth of the internet as a distributed medium, the metaverse is shaping up to be a corporate-controlled environment.[25] Companies are building closed-loop systems to control what companies and which users are allowed to access the system and play or work in those systems. Further, if multiple closed-loop systems, walled gardens, or insular VR app stores develop, they may not be interoperable for either the hardware or the software, similar to Apple's App Store and Google Play and their respective hardware. Bundling is one possible outcome, allowing users to access many environments (the "cable" model). It's also possible that competing environments will cater to different categories of users (the "channel" model). Where will government, public services, and education be situated in virtual reality or the metaverse? At the time of this report's publication, there is no legislation requiring the equivalent of "must carry" or public access to any metaverse system, but open and decentralized versions of the metaverse built on web standards have already been proposed.[26]

VR systems make money for their parent corporations by selling hardware and software, by selling advertising, and by gathering information about their users to offer additional products and services for commercial purposes. These systems also sell "access" to VR users' rich, sensitive personal information to third parties for research and commercial purposes. Much like current app stores, additional sources of revenue may include in-app purchases or in-world sales, and the resale of the data that VR devices collect from users in virtual reality to third parties.[27] Popular devices that have since entered the market include the Oculus Rift,[28] Samsung Gear VR,[29] HTC Vive,[30] Google Cardboard,[31] Google Glass,[32] Ray-Ban Stories,[33] and Snap Spectacles.[34]

Each of these early devices has attempted to hit a magical medium between being a lightweight and unobtrusive wearable device yet one with plenty of useful features. Each one has succeeded in some ways and failed in others. As yet, not one of these devices has become a tool necessary to interact with and function in society, like the smartphone or (in a previous era) the television and telephone. But this moment in time may come, so we need to examine these VR devices and their use in the metaverse to imagine what the user experience may be

[20] *See* footnote 19.

[21] Zhang, S., Feng, Y., Bauer, L., Cranor, L.F., Das, A., & Sadeh, N. (2020). 'Did you know this camera tracks your mood?': Understanding privacy expectations and preferences in the age of video analytics. *Proceedings on Privacy Enhancing Technologies* (2): 282–304. https://doi.org/10.2478/popets-2021-0028.

[22] Advertising in VR is immersive and pervasive. *See* Heller and Bar-Zeev, "The problems with immersive advertising: In AR/VR, nobody knows you are an ad," available at https://tsjournal.org/index.php/jots/article/view/21/10, for a discussion of "playable" ads.

[23] Surveillance capitalism is an economic practice centered around the commodification of personal data with the core purpose of profit-making. The term "surveillance capitalism" was popularized by the author Shoshana Zuboff in her book *The Age of Surveillance Capitalism*, published in 2019.

[24] Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2019). Privacy risks and harms. *Common Sense Media*. https://privacy.commonsense.org/content/resource/privacy-risks-harms-report/privacy-risks-harms-report.pdf.

[25] *See* Steam Hardware & Software Survey: May 2022, https://store.steampowered.com/hwsurvey/Steam-Hardware-Software-Survey-Welcome-to-Steam?platform=combined; Meta now has a dominant market share in virtual reality thanks to its 2014 acquisition of Oculus and its Quest VR headset.

[26] *See* Third Room: https://thirdroom.io.

[27] Even just sharing with affiliates opens a rather large market. "No matter which VR you're using, your data will be shared with network affiliates and subsidiaries." Hunt, C. (2018, November 21). VR and your privacy: How are these companies treating your data? *Windows Central*. https://www.windowscentral.com/vr-and-your-privacy-how-are-these-companies-treating-your-data.

[28] *See* Meta Quest, Oculus Rift: https://www.oculus.com/rift/setup.

[29] *See* Samsung Gear VR: https://www.samsung.com/us/support/mobile/virtual-reality/gear-vr/gear-vr-with-controller.

[30] *See* HTC Vive: https://www.vive.com/us.

[31] *See* Google Cardboard: https://arvr.google.com/cardboard.

[32] *See* Google Glass: https://www.google.com/glass/start.

[33] *See* Facebook Ray-Ban Stories: https://www.ray-ban.com/usa/ray-ban-stories.

[34] *See* Snapchat Spectacles: https://www.spectacles.com.

like if and when such devices are crucial to participation in the world of commerce, government, or education.

This series of virtual reality failures and missed opportunities puts pressure on even the largest companies to generate revenue with virtual reality at any expense. History tells us that the easiest way to do that is make the products cheap, popular at scale, and so appealing that everyone wants one, often at the expense of deep consideration of the privacy concerns and safety pros and cons of using such a device.

Given that our focus is privacy, we look primarily at the types and quantities of data that the devices collect on behalf of their corporate backers, and what they intend to do with the personal information that they collect. We do know, based on VR's potential to collect new categories of personal information,[35] including the user's sensory experiences, that we're delving into a new world of data collection beyond what previous, text-based interfaces could gather. For example, VR hardware and software may collect three-dimensional coordinates of the user's environment, head position, height, and location of users' head and arms in a 3D plane. It may also collect precise time information and data on normative body language, including gaze, facial expressions, emotional recognition[36], and such gestures as hand positions and movements with objects.[37]

In addition, web cameras and VR devices have the capability to scan a user's private physical space (such as their bedroom) and identify the objects within.[38] VR devices can also detect eye tracking, gaze detection, pupil dilation, and usage data, such as location-based information (time zone/country), behavioral data of interactions, as well as IP address, VR web browser activity,[39] and unique device identifiers.[40] Companies may use this sensitive personal information for their own commercial purposes to profile users based on their unique biometric data points, possibly resulting in unintended or even unimagined consequences.[41]

VR users provide a massive treasure trove of new information[42] to companies. In many cases, the technology may be gathering data not anticipated by privacy policies and laws written years or decades before such technology existed. Further, the policies, laws, and industry standards may encompass the technology but not contemplate the potential uses of the data collected by this technology and resulting risks to privacy.

Mask up: Personal privacy and identity risks

How should we discuss personal privacy risks in VR? We can begin by looking at the technical capacities of the devices and software. However, the psychological consequences of a new portal into reality may be far beyond just adding a new product to the lineup. Users may be entranced by the possibilities of using commercial products for educational purposes,[43] and using education products (intended to be used with supervision in a classroom) at home, and other unintended uses.[44] Behavioral modification derived from a user's virtual reality experiences can be positive, negative, or some combination of the two. Consider the example of using VR to moderate PTSD, or, conversely, having VR contribute to PTSD with

[35] Or maybe it's more than a bug, or even a feature. Maybe it's the core functionality: "But XR technologies typically cannot function without collecting sensitive personal information—data that can create privacy risks. Some VR and AR systems rely on biometric identifiers and measurements, real-time tracking of individuals' location, and precise maps of the physical world including the interiors of homes, offices, and medical facilities." Jerome, J., & Greenberg, J. (April 2021). Augmented reality + virtual reality: Privacy & autonomy considerations in emerging, immersive digital worlds. The Future of Privacy Forum. https://fpf.org/wp-content/uploads/2021/04/FPF-ARVR-Report-4.16.21-Digital.pdf.

[36] "Discrete functions of XR technology, such as facial or emotional recognition, could be unethically used to discriminate against individuals who are neurodivergent, have physical disabilities affecting their facial expressions, or come from cultures with physical expressions of emotion that vary from the expressions programmed into the facial recognition technology." Pahi, S., & Schroeder, C. *Extended privacy for extended reality: XR technology has 99 problems and privacy is several of them*. https://ssrn.com/abstract=4202913.

[37] Researchers refer to this type of nonverbal or biometrically inferred or derived data using a number of terms. Some are included in the XRSI Privacy Framework Version 1.0, XR Safety Initiative (September 2020), https://xrsi.org/publication/the-xrsi-privacy-framework.

[38] *See* Holpuch, A., & Rubin, A. (2022, August 25). Remote scan of student's room before test violated his privacy, judge rules. *New York Times*. https://www.nytimes.com/2022/08/25/us/remote-testing-student-home-scan-privacy.html.

[39] Kraus, F. (2022, August 10). *iOS privacy: Instagram and Facebook can track anything you do on any website in their in-app browser*. https://krausefx.com/blog/ios-privacy-instagram-and-facebook-can-track-anything-you-do-on-any-website-in-their-in-app-browser.

[40] "Data capture in VR is oftentimes a hidden feature of industry-oriented VR applications, but it is maybe one of the most important aspects… In fact, the data available in VR are tantamount to having a real person wear a GPS tracking device, speedometer, and a full-body sensor suit while they do a training session or some other activity." https://hellodarwin.com/blog/virtual-reality-data-collection.

[41] "Using Oculus's recent privacy policy as a case study, this Note shows how this hidden knowledge shift transforms the meaning of ordinary privacy policy phrases like 'experience unique and relevant to you.' What Oculus finds to be 'relevant' to the user could be beyond what the user themselves would imagine or notice to be 'relevant.' As a result, the text becomes an obsolete medium to communicate privacy risks to virtual reality users." From the abstract for Kim, Y. Virtual reality data and its privacy regulatory challenges: A call to move beyond text-based informed consent. *California Law Review*, https://www.californialawreview.org/print/virtual-reality-data-and-its-privacy-regulatory-challenges-a-call-to-move-beyond-text-based-informed-consent.

[42] Further, this information is not gathered and discarded, but stored in a variety of increasingly capacious cloud solutions. Jerome, J., & Greenberg, J. (April 2021). Augmented reality + virtual reality: Privacy & autonomy considerations in emerging, immersive digital worlds, pp. 9. The Future of Privacy Forum. https://fpf.org/wp-content/uploads/2021/04/FPF-ARVR-Report-4.16.21-Digital.pdf.

[43] Educational institutions have begun offering guides to using VR in an effort to make this product safe(r) for classroom use, see, e.g., https://guides.library.utoronto.ca/c.php?g=607624&p=4938314.

[44] *See* Lenovo VR Classroom: https://techtoday.lenovo.com/us/en/solutions/vr-classroom.

unexpected, disturbing imagery or abuse that a user not only sees, but also experiences.[45,46]

We don't yet know the long-term effects on kids, but current research indicates that kids likely experience virtual reality in a manner similar to physical reality.[47] At present, we run the risk of normalizing children's use of VR as harmless or just like interacting with existing media and games. However, more caution is warranted in VR. In VR, we need more careful consideration of what content and experiences kids are engaging with. It is also important to ensure that kids are interacting in spaces and engaging with content that is appropriately designed with their unique needs in mind.

Additionally, if interactions with other users are possible in VR spaces, methods need to be put in place to ensure those individuals are trustworthy. For children under 8 who are unable to determine when other people have their best interests in mind,[48] engaging with VR experiences is more likely to create harmful experiences or present situations that they are not developmentally prepared to navigate. For this reason it is our recommendation that all kids, including teens, do not engage with VR devices and content unless parents and caregivers have carefully reviewed and continually help their children reflect on the interactions and experiences they encounter. This increases the likelihood that any VR experiences with children are appropriate and beneficial for their development.

For teens, interactions in VR require more nuance and consideration of their individual capabilities and needs. We must consider that as kids get older, they will need autonomy to learn and make mistakes with minimal or no adult supervision. This also includes the freedom to make decisions and not have a permanent record that shapes and limits future opportunities and experiences. Engaging in interactive experiences that present more risk can also present more opportunities for positive experiences,[49] but those experiences should be developmentally appropriate to ensure that teens have the skills necessary to navigate both positive and negative experiences in a manner that is safe, beneficial, and appropriate. We should prepare teens to navigate their safety and know how to stop unwanted virtual interactions or content. We should encourage them to reflect on their experiences to help minimize the potential for social or emotional harm.

There's also a lack of age gating in VR, which creates risks for children to be exposed to inappropriate or even criminal behavior. Teens are likely to engage in more social aspects or interact with untrusted users in a given VR environment and they should be aware that their voices and other behavior can give away detailed information about themselves and their identity, such as their likely age, ethnicity, race, education, or even general locale (based on accent). Young people need to learn how to use technology to control how, and what, information they share about themselves, because it is an important set of skills to develop to ensure virtual spaces we interact with are beneficial. Anonymity in VR is just as important to teens and other vulnerable communities as anonymity in other online spaces, and users should be able to hide their identity by creating avatars and masking their voice by default without having to use complicated third-party apps with different privacy practices.

Of course, as with any technology, there is the possibility of addictive behavior, but VR might enhance that possibility by offering a more pleasurable and immersive experience than reality—a true alternative to reality to express one's thoughts and desires. The cost-benefit analysis of this technology may continue, but for now, we need to know the immediate impact on kids and their privacy.

With these privacy concerns in mind, we should know what we're getting into when we enter virtual reality and the metaverse. We begin by looking at the current devices available to ascertain which companies have entered the market and what methodologies they use to access the metaverse. Only by understanding the actual privacy practices of the most popular VR devices and the promises that companies make in these policies will it be possible for society to create a virtual reality world where everyone's privacy is better protected.

Children and data privacy

When it comes to their children and students, parents and educators value the ability to understand and control what personal information is collected from the apps and devices their children use. However, do parents and caregivers know how to control what information is collected, and whether their child's or students' personal data is being used to deliver personalized or targeted ads? Parents need to know virtual reality apps and devices can request access to a much wider range of sensitive data than other devices (such as location), and can

[45] Scary and traumatic experiences are unfortunately common in XR. *See* Blum, D. (2021, June 3). Virtual reality therapy plunges patients back into trauma. Here is why some swear by it. *New York Times*. https://www.nytimes.com/2021/06/03/well/mind/vr-therapy.html.

[46] "Almost as soon as social VR came into being, reports of abuse of users in the experiences followed." Heller, B. (2020, June 12). Reimagining reality: Human rights and immersive technology, pp. 10. *Carr Center Discussion Paper Series*. https://carrcenter.hks.harvard.edu/publications/reimagining-reality-human-rights-and-immersive-technology.

[47] Jerome, J., & Greenberg, J. (April 2021). Augmented reality + virtual reality: Privacy & autonomy considerations in emerging, immersive digital worlds; initial effects, pp.11; long-term effects, pp. 12–13. The Future of Privacy Forum. https://fpf.org/wp-content/uploads/2021/04/FPF-ARVR-Report-4.16.21-Digital.pdf.

[48] Wilcox, B., Kunkel, D., Cantor, J., Dowrick, P., Linn. S., & Palmer, E. (2004, February 20). Report of the APA task force on advertising and children. APA. https://www.apa.org/pi/families/resources/advertising-children.pdf.

[49] Risks and opportunities described in Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., and Hasebrink, U. (2020). "EU Kids Online 2020: Survey results from 19 countries. EU Kids Online." https://doi.org/10.21953/lse.47fdeqj01ofo

display age-appropriate or age-inappropriate media as well as install third-party apps and games. Parents and educators also may feel like they don't have the ability to make a meaningful choice when it comes to privacy because the third-party apps, games, and content they need in virtual reality is available only for a single virtual reality device or app.

- **The facts**: Virtual reality apps and devices can collect a significant amount of sensitive, behavioral, and personal information that could be used in unintended ways, causing social or emotional risks. Current VR headsets and body-tracking systems collect and share a user's sensitive data with each third-party VR app a user downloads. Unlike a mobile app or device, 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 including posture, eye gaze, pupil dilation, gestures, and facial expressions.[50]
- **The feelings**: Parents and educators may have feelings about virtual reality apps and devices always collecting data from their children and students while they are using the device to create a personalized profile—basically every movement or interaction. This is often referred to as the "creepiness" factor and could include collecting behavioral data without express permission, or using the data for purposes other than what the device was initially used for. For example, a person might use a virtual reality device and then all the data captured about their bodily movements, social interactions, eye tracking, and usage interactions could be used to manipulate what content they see over time on other applications and services across the internet.
- **The cost**: Virtual reality devices are cost prohibitive for most kids and families, especially for lower-income households. In addition, VR devices are also still too expensive for most schools and districts to incorporate into their computer labs, except for specialized STEM and esports programs. This creates an access and equity issue, similar to the digital divide, in which a lack of high-quality internet access[51] at home can put kids at a disadvantage when their education, schoolwork, entertainment opportunities, and social communication with friends and family requires access to the internet.

  In addition to the cost of internet access, wireless VR devices cost hundreds of dollars each, and most wired VR devices also require a modern personal computer with software that can cost thousands of dollars, which also must also have a powerful graphics card that can cost hundreds of dollars. All this technology is required to connect a wired VR device to a personal computer, the internet, a VR app, and display the 3D experience. Moreover, third-party VR apps, games, and software experiences must all be purchased separately, which can increase the total cost of VR ownership over time.

  All together, VR is not currently affordable or accessible to the majority of U.S households, which could further entrench and widen the digital divide for kids from lower socioeconomic backgrounds, so they would have no knowledge or experience with emerging new technologies like VR until long after their peers. Lack of access and the opportunity to learn about the beneficial uses of technology may present knowledge gaps for kids if VR one day becomes as ubiquitous as personal computers and mobile phones.
- **The future**: Beyond what is currently collected and how it is used, virtual reality devices and third-party VR apps may store all the data they collect indefinitely. At some point, companies may use the data in ways that no one has yet imagined, such as changing default interactions on other unrelated apps and services based on what types of social interactions or bodily movements a user had in virtual reality years before.

  In addition, data brokers could combine a user's anonymized behavioral data with data collected from other apps and services, which may allow the anonymized data to be re-identified. Data could also be further analyzed to derive a user's emotional state or their perceptibility to persuasion for commercial purposes. With children, the impact is magnified by time because data collected in childhood can follow people into adulthood. We currently consider data collection and processing of data from children, but we also need to imagine how data collected now will be used in the future as individual data points contribute to data profiles. To that end, the Common Sense Privacy Program has applied its hardware and software evaluation methodology to this new technology of virtual reality.

[50] Bailenson, J. (2018). Protecting nonverbal data tracked in virtual reality. *JAMA Pediatr*. 172(10): 905–906. https://stanfordvr.com/pubs/2018/protecting-nonverbal-data-tracked-in-virtual-reality/.

[51] *See* Chandra, S., Chang, A., Day, L., Fazlullah, A., Liu, J., McBride, L., Mudalige, T., & Weiss, D. (2020). Closing the K–12 digital divide in the age of distance learning. *Common Sense Media and Boston Consulting Group*. https://www.commonsensemedia.org/sites/default/files/featured-content/files/common_sense_media_report_final_7_1_3pm_web.pdf.

The next virtual frontier

As compared to existing technologies, such as web browsers, apps, and mobile devices, virtual reality devices can collect exponentially more data points about an individual. Over time, this intimate data about body movements, emotions, preferences, and behaviors can be used to create a "digital signature" that uniquely represents a user's sensitive biometric information and is as personally identifiable as a fingerprint. AR also has the potential to create a future "mirror world" where information overlays practically every real world object and also lets users interact with, manipulate, and experience shared virtual objects and experiences all around us like we do the real world.[52] As we think about what the next technology or virtual frontier will look like, we also need to consider how expectations of privacy and privacy protections will need to change as a result of VR's or AR's unique capabilities, and how to disclose the new types of data collected.[53] Hopefully the facts presented in this report will elucidate the many privacy risks in VR for kids and families at this critical moment in the development of a new technology, and help society confront these challenges head on.

[52] Kevin Kelly. (Feb 12, 2019). AR Will Spark the Next Big Tech Platform—Call It Mirrorworld. *Wired*. https://www.wired.com/story/mirrorworld-ar-next-big-tech-platform.

[53] *See* Trimananda, R., Le, H., Cui, H., Ho, J.T., Shuba, A., & Markopoulou, A. (2021). OVRseen: Auditing network traffic and privacy policies in Oculus VR. https://doi.org/10.48550/arXiv.2106.05407.

How we rate privacy

Privacy and security are intertwined, and security is the foundation of effective individual privacy. When evaluating whether to have children or students use virtual reality devices at home or in the classroom, parents and teachers need to understand both the privacy policies and security practices of the device. To create a truly comprehensive evaluation process, the Common Sense Privacy Program completes a full, in-depth, 150-point inspection[54] of a product's privacy policies in order to offer privacy ratings[55] that are easy to understand.

Our privacy policy evaluation process attempts to address some common barriers to understanding a product's privacy practices. The process includes questions organized into categories and sections derived from the Fair Information Practice Principles[56] that underlie international privacy laws and regulations. The full evaluation questions and the categories that organize them are all mapped to a range of statutory, regulatory, and technical resources that provide background information on why each question is relevant to the privacy evaluation process.

In addition, every product with a privacy rating includes an overall evaluation score.[57] A higher score (up to 100%) means the product provides more transparent and comprehensive privacy policies with "better" practices to protect user data. The overall score is not an average of the evaluation concern[58] category scores, but rather is a percentage of the number of points earned for 28 basic evaluation questions. The score is best used as an indicator of how much additional work a person will need to do to make an informed decision about a product. This use is directly related to the core principle driving the evaluations—to help people make informed decisions about a product or service with less effort. The higher the number, the less effort required to make an informed and appropriate decision.

Virtual reality devices we rated

In order to better understand the privacy practices of virtual reality (VR), augmented reality (AR), and the metaverse, we purchased and tested the most popular virtual and augmented reality devices on the market to identify the potential privacy risks and harms that may affect the consumers, children, students, and families who use these devices. Currently there are not very many virtual reality devices to choose from, with only about a dozen major companies competing with similar features at different price points.[59]

We selected the top seven devices from companies representing close to 100% of the current market. We believe these seven devices are representative of most types of virtual reality and augmented reality devices and platforms available today.[60] We chose devices based on the company, product features, app stores, interoperability, price, and popularity. We also chose virtual reality and augmented reality devices used for gaming, business, and education that are used by consumers, children, teens, and students in every major age group at home and in the classroom. We tested the following seven devices:

HP Reverb G2

Figure 1: Image of HP Reverb G2

[54] *See* Common Sense, Evaluation Questions: https://privacy.commonsense.org/resource/evaluation-questions.

[55] *See* Common Sense Privacy Ratings: https://privacy.commonsense.org/resource/privacy-ratings.

[56] The Fair Information Practice Principles (FIPPs) are a set of eight principles that are rooted in the tenets of the Privacy Act of 1974; *see* Privacy Act of 1974, 5 U.S.C. § 552a.

[57] *See* Common Sense Privacy Program, Evaluation Scores: https://privacy.commonsense.org/resource/evaluation-scores.

[58] *See* Common Sense Privacy Program, Evaluation Concerns: https://privacy.commonsense.org/resource/evaluation-concerns.

[59] Fortune Business Insights. (May 2022). *Virtual reality market size, share, & COVID-19 impact analysis, by component (hardware, software, content), by device type (head mounted display, VR simulator, VR glasses, treadmills & haptic gloves, others), by industry (gaming, entertainment, automotive, retail, healthcare, education, aerospace & defense, manufacturing, others), and regional forecast.* https://www.fortunebusinessinsights.com/industry-reports/virtual-reality-market-101378.

[60] *See* footnote 25.

The HP Reverb G2[61] is a virtual reality wired headset that was developed in collaboration with Valve and Microsoft. It delivers an immersive, comfortable, and compatible experience with the SteamVR software distribution platform. The Reverb G2 has one of the highest VR resolutions on the market, which makes it a great choice to use with simulation VR apps. The headset looks similar to the *Valve Index* headset but has distinct Microsoft hand controllers with a Windows button on the controllers for better interaction with Microsoft Mixed Reality experiences and applications. The device is aimed at business or enterprise customers and supports integration with both the SteamVR marketplace and the Windows Mixed Reality environment. Users can download and use Mixed Reality productivity-focused desktop applications to browse the web with Microsoft Edge or work with Microsoft Office applications in VR to enhance collaboration, communication, and productivity.

HTC Vive Cosmos Elite

Figure 2: Image of HTC Vive Cosmos Elite

The HTC Vive Cosmos Elite[62] is a virtual reality wired headset that provides an immersive experience and integrates with SteamVR's tracking system[63] to keep track of the user's orientation in their real-world environment. The device includes stereo audio integrated into on-ear, form-fitting headphones. The Vive is compatible with software distribution platforms such as SteamVR and HTC's Viveport personal computer software. The Cosmos Elite uses distinct handheld controllers and its faceplate flips up in a unique feature that allows views of the real world quickly and easily without having to completely take off the headset. An optional wireless adapter allows for greater movement in VR by eliminating the requirement to be tethered to the user's personal computer with a cable. The Cosmos Elite is aimed at a general consumer audience with various software categories in its Viveport Store that include streaming media content, apps, games, education, and productivity.

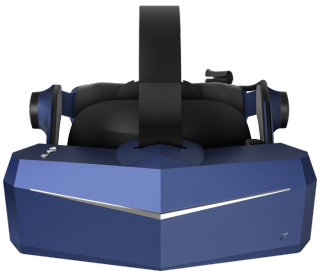
Figure 3: Image of Meta Quest 2

Meta Quest 2

The Meta Quest 2[64] (formerly known as Oculus Quest 2) is a wireless virtual reality headset developed by Facebook Reality Labs (formerly Oculus). The Quest 2 is the most popular virtual reality headset on the market today, and its low cost is aimed at a general consumer audience with optional social network account integration into Meta's Facebook. The Quest 2 is capable of being used as both a standalone wireless headset or connected to a desktop computer over a USB cable or Wi-Fi with Airlink software. The Quest 2 has touch controllers and features "inside-out" tracking using the cameras and computer vision algorithms to map the surrounding real-world environment.[65] The Quest 2 software distribution platform is limited to the Meta App Store on the device itself and Oculus VR software running on a user's personal computer. The optional personal computer USB cable and Airlink option expands the catalog of available VR applications, content, and games and additional third-party add-ons allow integration with content from SteamVR.

Pimax Vision 5K Super

Figure 4: Image of Pimax Vision 5K Super



The Pimax Vision 5K Super[66] is a wired virtual reality headset primarily designed for esports and gaming

[61] *See* HP Reverb G2: https://www.hp.com/us-en/vr/reverb-g2-vr-headset.html.
[62] *See* HTC Vive Cosmos Elite: https://www.vive.com/us/product/vive-cosmos/overview.
[63] *See* SteamVR Tracking: https://partner.steamgames.com/vrlicensing.
[64] *See* Meta Quest 2: https://www.oculus.com/quest-2.
[65] *See* Heaney, D. (2019, April 29). How VR positional tracking systems work. *UploadVR*. https://uploadvr.com/how-vr-tracking-works.
[66] *See* Pimax Vision 5K Super: https://pimax.com/product/vision-5k-super.

because of its ultrawide, 200-degree field of view that allows the user to see more of their virtual environment for a more immersive experience. In addition, the device's high resolution and high refresh rate make it appealing to VR enthusiasts looking for the best possible hardware specifications who also want to tweak their custom VR settings with more options. The device requires the personal computer software tool Pitool to be installed for configuration, but completely integrates with SteamVR or the Oculus desktop app to access VR-related content.

PlayStation VR

Figure 5: Image of PlayStation VR

The PlayStation VR[67] is a wired headset natively compatible with the PlayStation 4 console (and PlayStation 5 console with an additional adapter). The device is intended only for use with compatible VR titles purchased through the PlayStation VR Store. The headset is tethered to the PlayStation console and requires an additional hardware unit attached to the PlayStation 5 to connect the device. The headset uniquely uses an OLED screen with in-ear wired headphones and can use DualShock wireless controllers[68] or distinct move motion controllers[69] in VR. The device is intended only for a gaming audience and uses a forward-facing PlayStation camera tracking system to control the VR experience, which can cause tracking issues if the user is not directly facing the camera.

Valve Index

The *Valve Index*[70] is a virtual reality wired headset created and manufactured by Valve, which also owns the software distribution platform Steam and SteamVR headset software. The headset and controllers both support Valve's VR tracking system and the Index includes custom controllers and off-ear headphones. The Index is

Figure 6: Image of Valve Index

compatible with SteamVR and any VR title a user purchases on Steam is playable on any other SteamVR compatible VR headsets, such as the HTC Vive, Oculus Rift, and Mixed Reality headsets. The Index is aimed at a gaming audience looking for an all-around best-in-class agnostic VR device with easy SteamVR integration bundled with a free copy of the game Half Life: Alyx at the time of purchase.

Microsoft HoloLens 2

Figure 7: Image of Microsoft HoloLens 2

The Microsoft HoloLens 2[71] is an augmented reality headset, which means it uses see-through holographic lenses which project holographic images into the user's real-world environment. The user is able to see both their real-world environment and the augmented environment as an additional "layer" on top of the real world, in real time. The HoloLens has built-in spatial sound and uses hand tracking with direct manipulation of holographic images in midair with real-time eye tracking. The device uses world-scale positional tracking and is built on a Mixed Reality version of the Windows holographic operating system that uses the Microsoft App Store to download and purchase HoloLens specific applications. The HoloLens is aimed at a business, education, or enterprise audience with limited app store industry specific categories of applications.

[67] *See* PlayStation VR: https://www.playstation.com/en-us/ps-vr.
[68] *See* DualShock 4 Wireless Controller: https://www.playstation.com/en-us/accessories/dualshock-4-wireless-controller/.
[69] *See* PlayStation Move Motion Controller: https://www.playstation.com/en-us/accessories/playstation-move-motion-controller/.
[70] *See* Valve Index: https://www.valvesoftware.com/en/index.
[71] *See* Microsoft HoloLens 2: https://www.microsoft.com/en-us/hololens.

Virtual reality device specifications

Table 1 shows the technical specifications of the most popular virtual reality headsets that were tested for this report. There are two primary categories of virtual reality devices: 1) Wireless devices—which are standalone devices that have all the necessary software components to provide virtual reality experiences integrated into the headset, and 2) Wired or tethered devices, which are headsets that serve as a display device for another computing device, like a PC or a video game console, that provides the software for the virtual reality experience. VR headsets also use technologies and terms such as LCD or OLED to refer to the type of lenses and display, and cameras mounted on the device or outside the device to refer to inside-out or outside-in tracking that determine the position of the user in the VR environment.

Table 1: Virtual reality device specifications

	Microsoft HoloLens 2	HP Reverb G2	HTC Vive Cosmos Elite	PlayStation VR	Meta Quest 2	Valve Index	Pimax Vision 5K Super
Type	AR	VR	VR	VR	VR	VR	VR
Connection	Wireless	Wired to PC	Wired connection to PC (wireless add-on available)	Wired connection to console	Wireless with optional Cable/ AirLink	Wired connection to PC	Wired to PC
Price	$3,500	$599	$699	$299	$299	$999	$689
Display Per Eye	1280 × 720	2160 x 2160	1440x1700	1920 x 1080	1832 x 1920	1440 x 1600	2560 x 1440
Display Type	Holographic	LCD	LCD	OLED	LCD	LCD	LCD
Pixels Per Degree	~20	18.95	13.09	9.6	20.5	11.07	21.33
Refresh Rate	60Hz	90Hz	90Hz	90/120 Hz	71/90/120Hz	90/120/144Hz	90/120/144/ 160/180Hz
Tracking Type	World-scale positional tracking	4 camera inside-out	Inside-out markerless	Outside-in via the PlayStation Camera	4-Camera Oculus Insight	Outside-in via 2 – 4 SteamVR base stations	Inside-out markerless
Field of View	52 degrees	114 degrees	110 degrees	100 degrees	89 degrees	130 degrees	200 degrees
Eye Tracking	Yes	No	No	No	No	No	Yes (optional)
Hand Tracking	Yes	No	Yes	No	Yes	No	Yes
Microphone	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audio	Built-in spatial sound	Off-ear speakers	Integrated headphones	1x 3.5 mm audio jack	Integrated headphones	Off-ear speakers, 3.5 mm audio jack, built-in microphone	Integrated headphones
Controllers	Two-handed direct manipulation	Bundled Windows MR controllers with sticks, buttons, triggers, grip	Bundled Vive wands with trackpad, triggers, grips	Bundled Sense controllers with buttons, sticks,	Touch controllers	Bundled Valve Index controllers with touch sensing for all fingers/thumbs, sticks, buttons, triggers, trackpad	Extra Sword controllers
Weight	566 g	499 g	702 g	600 g	571 g	809 g	514 g
Platform	Mixed Reality, Microsoft Store	SteamVR, Mixed Reality	SteamVR, HTC Viveport	PS4, PS5	Meta App Store, Oculus App	SteamVR	SteamVR, Pitool

Privacy Results

We read and evaluated the public privacy policies of all virtual reality devices tested in this report to determine their data collection and use policies. In Table 2, "Yes" is considered a worse practice compared to what better privacy practices a company should disclose in their privacy policy. Worse practices can put children, students', and consumers' privacy at risk. Our privacy evaluations of the most popular virtual reality devices indicate that all devices received a "Warning" rating, which means they all have worse privacy practices that put consumers' privacy at considerable risk by exploiting the sensitive behavioral data of users for profit. All of the virtual reality devices state in their privacy policies that they can use sensitive biometric data collected in virtual reality for commercial purposes that include selling their data to third parties, sending users third-party marketing communications, displaying targeted advertisements, tracking users across other sites and services over time, and creating advertising profiles for data brokers.

None of the most popular virtual reality headsets have earned our recommendations for kids and families.

The following evaluation questions are used to rate the privacy practices of VR devices and applications.

Sell data

The sell data evaluation question indicates whether the VR device or application's policies disclose whether a user's personal information is sold or rented to third parties for monetary or other valuable consideration. Selling users' data for profit is an important issue for consumers and should be disclosed in a developer's privacy policy because users want to know if their data is shared with third parties for profit in exchange for their use of the product, which may influence their decision whether to use the product or service or allow their children or students to do so.[72,73,74,75,76,77]

Third-party marketing

The third-party marketing evaluation question indicates whether marketing communications that could include emails, text messages, or other app notifications are sent to users of a VR device or application from a third-party application or service that a user does not have a direct relationship with. These marketing communications typically are unexpected and unwanted by users because they use their personal information to communicate unrelated or unsolicited products and services from third-party companies.[78,79,80,81,82,83]

Personalized ads

The personalized advertising evaluation question indicates whether advertisements are displayed to any users based on collected personal information or behavioral information on how users use the VR device or app, also known as behavioral or targeted advertisements. Personalized advertisements take targeted advertisements one step further, collecting specific information about users typically through the use of cookies, beacons, tracking pixels, persistent identifiers, or other

[72] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2..
[73] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(3).
[74] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.120(b)-(c).
[75] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.135(a).
[76] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(ad)(1).
[77] *See* General Data Protection Regulation (GDPR), Art. 13(2)(b), 14(2)(c), 15(1)(e), 18(1)(d), 21(1), 21(4).
[78] *See* footnote 72.
[79] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(1)(A).
[80] *See* California Privacy Rights for Minors in the Digital World, Cal. B.&P. Code §§ 22580-22582.
[81] *See* Shine the Light, Information Sharing Disclosure, Cal. Civ. Code §§ 1798.83-1798.84.
[82] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(a).
[83] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(e)(6).

tracking technologies that provide more specific information about the user's preferences and characteristics. This information is often shared with third-party advertisers, who display even more personalized products and services than targeted advertisements to the user, based on the specific information they received from the user's activities on the product.[84,85,86]

Third-party tracking

The third-party tracking evaluation question indicates whether the developer allows third-party companies to use cookies or other tracking technologies on its product, which enables those third-party companies to collect and use personal information for their own purposes. Best practice is to not permit third-party advertising services or tracking technologies to collect any information from a user while using the service. A user's personal information provided to a product also should not be used by a third party to persistently track that user's behavioral activity on the product in order to influence what content they see in the product and elsewhere online. Third-party tracking can influence a user's decision-making processes without their knowledge, which may cause unintended harm.[87,88,89]

Track users

The track users evaluation question indicates that the product uses cookies or other tracking technologies on its service for the specific purpose of allowing third-party companies to display advertisements to the developer's users on other apps and services across the internet. Best practice is to not track users to target them with advertisements on other third-party websites or services. A user's personal information provided to a product should not be used by a third party to persistently track that user's behavioral actions over time and across the internet on other apps and services.[90,91,92,93,94]

Ad profile

The ad profile evaluation question indicates that a product allows third-party companies to create a behavioral profile about a user, based on the user's personal information or activity for advertising or marketing purposes across the internet. A developer should not allow third parties to create a profile from a user's personal data, engage in data enhancement, or target advertising based on that profile. Automated decision-making, including the creation of profiles for tracking or advertising purposes, can lead to an increased risk of harmful outcomes that may disproportionately and significantly affect children or students.[95,96,97,98,99]

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

What we found

The *Microsoft*, *HP*, *PlayStation*, and *Meta* privacy policies all say they do not sell a user's data to third parties, which is initially promising because it is a better privacy-protecting practice for kids and families. However, new state privacy laws, like the California Consumer Privacy Act, (CPRA)[100] are expected to expand what "selling data" means to include additional types of data monetization methods, like tracking and targeted advertising. The "sell data" rating criteria was the only issue where companies indicated a "better" practice that they do not engage in selling data of users to third parties, but they still use users' data for other commercial purposes such as third-party marketing, targeted advertising, or tracking. This inconsistency may be explained by the limitation of the definition of "sale" in the current California Consumer Privacy Act (CCPA).[101] Therefore, *Microsoft*, *HP*, *PlayStation*, and *Meta* will likely soon need to change their privacy policy to say that they actually sell users' data for profit under new state privacy laws.[102] Only *HTC* was explicitly transparent in their privacy policy that they already engage in the "worse" practice of selling users' data to third parties for profit.

[84] *See* footnote 72.
[85] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(e)(6), (ah).
[86] *See* footnote 79.
[87] *See* footnote 72.
[88] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(7).
[89] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.140(k), (l), (ah), (aj).
[90] *See* footnote 72.
[91] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.1.
[92] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(1)(B).
[93] *See* footnote 80.
[94] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.140(e)(4), (k), (ah), (aj).
[95] *See* footnote 72.
[96] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §§ 22584(b)(2), 22584(e)(2).
[97] *See* footnote 80.
[98] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.140(e)(4), (v)(1)(K), (z), (aj).
[99] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.8.
[100] *See* The California Privacy Rights Act of 2020, Proposition 24, in the November 3, 2020, General Election: https://thecpra.org.
[101] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100-1798.198.
[102] Common Sense Privacy Program. (2022, March 29). *A majority of apps are about to come clean and say they've been selling your data all along*. https://www.commonsense.org/education/articles/a-majority-of-apps-are-about-to-come-clean-and-say-theyve-been-selling-your-data-all-along.

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.

In addition, the policies of *Microsoft*, *HP*, *HTC*, *PlayStation*, and *Meta* all say they may send third-party marketing communications for other products and services to users, they may display targeted advertising to users while using the VR device or companion software, and may track users on the device and across the internet on other apps and services for commercial purposes.

The *Pimax* device is clear that its users' data can be used for third-party marketing and targeted advertising, but is unclear on all the other rating factors, which means Pimax may still engage in these worse monetization practices but without notice to users. Only *Valve* is unclear on all of our rating criteria in their policy, which indicates they likely are completely unaware of how important these privacy practices are to their users, which include parents, educators, and consumers. When a company is non-transparent in their policies about critically important privacy practices, such as the use of data for commercial purposes, there can be no future expectation or promise of how they will use data they collect from users in VR. Lastly, it is unclear from their policies whether *PlayStation*, *Valve*, or *Pimax* use a user's personal data to create an advertising profile to share with data brokers for commercial purposes, but it is likely that all three *PlayStation*, *Valve*, and *Pimax* devices engage in this additional type of monetization with VR users' data. [103]

Users need to know that what happens on their VR device does not stay on their VR device.

[103] *See* Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2021). State of Kids' Privacy 2021. *Common Sense Media*. https://www.commonsensemedia.org/research/state-of-kids-privacy-report-2021.

Compare privacy ratings

Table 3 compares the privacy practices of all the VR devices we tested, as described in their privacy policies. These practices can put children's and students' privacy at risk if they sell personal data to third-party companies or use personal information for third-party marketing, targeted advertising, tracking, or ad-profiling purposes. In addition, Table 3 illustrates a range of privacy practices from "best" to "poor" based on our privacy ratings and evaluation concerns. Products that score a "poor" are not necessarily unsafe, but they have a higher number of privacy problems than a product with a score of "average." Similarly, products that score "best" are not necessarily problem free, but they have relatively fewer problems compared to other products.

The evaluation concerns summarize the policies of an application or service into categories, based on a focused subset of evaluation questions that can be used to quickly identify the strengths and weaknesses of a company's policies. Ten different concerns have been created, based on feedback from consumers, parents, and educators on the most important questions they have about a product's privacy practices. Each concern is composed of eight to 10 of the most important evaluation questions related to the respective category. These concern categories provide a more comprehensive analysis and understanding of an application or service's strengths and weaknesses with respect to the specific concern and other products. The privacy evaluation concerns are identified by two-word question descriptions used to provide a general understanding of the topics covered by each concern. Each concern has its own concern score, which is calculated as a percentage given the number of questions in each concern.

- The concern category of data collection indicates whether the product has responsible data collection practices that limit the type and amount of personal information collected about users to only what's necessary to provide the application or service.
- The data sharing concern category indicates whether the product has data sharing best practices that protect a person's personal information from being shared with third-party companies and advertisers.
- The Data Security concern category indicates whether the product has data security best practices that protect the integrity and confidentiality of a person's data.
- The Data Rights concern category indicates whether the product provides the ability for users to exercise their data rights that include the ability to review, access, modify, delete, and export their personal information and content.
- The Individual Control concern category indicates whether the product allows users to exercise control over what personal data companies collect from them and to prevent its use for incompatible purposes.
- The Data Sold concern category indicates whether the product shares, rents, or sells a person's personal information to third parties for monetary value or other financial gain.
- The Data Safety concern category indicates whether the product limits the visibility of a person's information and their interactions with others to protect their physical and emotional well-being.
- The Ads & Tracking concern category indicates whether the product provides responsible advertising practices that limit the use of personal information for any third-party marketing, targeted advertising, tracking, or profile generation purposes.
- The Parental Consent concern category indicates whether the product is intended for children age 13 or under, and if a parent or guardian's verifiable consent is required before the collection, use, or disclosure of the child's personal information to an application or service.
- The School Purpose concern category indicates whether the product collects data from K–12 students and how the company follows federal and state legal obligations for the privacy and security of that educational information.

Table 3: Top virtual reality device privacy ratings and concern categories. Score Key: Best (81–100); Good (61–80); Average (41–60); Fair (21–40); Poor (0–20)

Product	Privacy Rating	Data Collection	Data Sharing	Data Security	Data Rights	Data Sold	Individual Control	User Safety	Ads & Tracking	Parental Consent	School Purpose
Microsoft HoloLens 2	75% Warning	Good	Best	Best	Best	Average	Best	Good	Good	Good	Average
HP Reverb G2	63% Warning	Good	Best	Average	Good	Average	Good	Poor	Average	Average	Poor
HTC Vive Cosmos Elite	63% Warning	Average	Good	Average	Best	Fair	Average	Fair	Good	Fair	Poor
PlayStation VR	59% Warning	Good	Good	Average	Average	Fair	Fair	Good	Average	Good	Poor
Meta Quest 2	55% Warning	Average	Best	Poor	Good	Fair	Fair	Average	Average	Fair	Poor
Valve Index	50% Warning	Average	Good	Fair	Best	Average	Fair	Average	Fair	Good	Poor
Pimax Vision 5K Super	30% Warning	Fair	Fair	Poor	Fair	Poor	Poor	Poor	Fair	Fair	Poor

Data Collection & Data Sharing

Microsoft has the highest Data Collection category scores, which indicates they are most transparent in their policies about the type of data they collect and whether they limit the collection of data to only the data necessary to provide the service. *PlayStation*, *HTC*, and *Valve* all score low on the Data Sharing category because they all have worse privacy-protecting practices when sharing users' data with third parties, and are nontransparent about several data sharing practices that are important to understanding how they use data collected in virtual reality.

Data Security & Data Rights

Microsoft scores highest in the Data Security category with Meta scoring the lowest, but overall most companies do not score well when it comes to security. *Microsoft's* policies clearly disclose all the protections they take to secure users' personal information. However, many of the other companies, including *Meta*, do not disclose any of their data security practices, which is cause for concern if these companies are not even taking reasonable measures to protect their users' data. *PlayStation* received the lowest score in the Data Rights category with all other companies scoring relatively high. Users expect to be able to access, modify, delete, and export their personal information from the company at any time. These privacy rights are required to be provided to users in various federal, state, and even international privacy laws, and even if *PlayStation* does provide these rights to users through its services, it also needs to disclose whether users have those rights in its privacy policy.

Data Sold

Microsoft has the highest scores in the Data Sold category, which looks at different ways companies can monetize user data. However, *Microsoft's* relatively high scores, as compared to other companies in this category, are still considerably low, and there are several issue areas they still need to improve with more transparency in their policies. Several other companies score very low in this category, but *PlayStation* and Meta have the lowest scores, which is unfortunate but not unexpected, given these virtual reality device manufacturers explicitly disclose that they share users' data with third parties for profit.

User Safety

PlayStation and *Microsoft* have the highest scores in the User Safety category, which is likely because both companies provide gaming services and provide extensive privacy settings and safety controls for their users that allow them to decide how and when they share information and communicate with other users. The *HP Reverb G2* has the lowest User Safety category score, which is likely because the company's virtual reality device is targeted more toward business and enterprise audiences, and *HP* likely assumes existing company appropriate use policies will ensure safer interactions. However, relying only on corporate policies to determine appropriate safety use is not an industry best practice because not disclosing safety practices for all users could be harmful to children, students, or consumers who use the VR device and have no safety protections or controls to avoid harassment or abuse.

Individual Control

Microsoft and *HP* have the highest scores in the Individual Control category because their policies disclose the purpose for which data in VR is collected and used as well as include privacy controls for users (such as opt-out), and indicate whether consent is required if a user's data is collected for a different context. The other virtual device companies did not transparently disclose how they provide users with control of their data, which indicates a user's data or even a bystander's data that is collected can be used for any unrestricted purpose.

Ads & Tracking

Microsoft and *HTC* have the highest scores in the Advertising and Tracking category because their policies transparently disclose whether they use personal information for targeted advertising, tracking across other sites and services, or using data for profiling purposes. However, *Valve* received the lowest score in this category because they did not transparently disclose any of their advertising or tracking practices in their policies, which provides no expectation or promise of how *Valve* will use personal information collected from its users in virtual reality.

Parental Consent

Valve, *Microsoft*, and *PlayStation* also received the highest scores in the Parental Consent category for disclosing all the different protections they provide to children under 13 and how parents can provide consent for the collection, use, and disclosure of their child's personal information. *Valve*, *Microsoft*, and *PlayStation* received high scores in the Parental Consent category because these companies provide gaming services and provide extensive privacy settings and safety controls that include robust parental controls and child user accounts. Among the VR devices we tested, *Valve*, *Microsoft*, and *PlayStation* are also the only companies that include children younger than 13 as an intended audience.

School Purpose

When it comes to use of virtual reality devices by students in K-12 schools and districts, only *Microsoft* provides substantive details in its policies about how it protects student data privacy. All other virtual reality device companies did not provide any information about

how they protect student data privacy when used in K–12 schools and districts in the School Purpose category. Use of virtual reality devices in schools or districts for educational purposes that require students to view documentaries or learning tutorials as part of a curriculum are typically outside the scope of the terms of use and license agreement of many virtual reality companies.

In addition, many companies disclose that users under 13 years of age are prohibited from using the virtual reality device, but this leaves students older than 13 who are authorized to use a company's device without any additional privacy protections. This may change as virtual reality companies realize that their products are being used more and more in lesson plans at home and by students in the classroom. It is recommended that school or district administrators, technology coordinators, or implementation specialists who would like to use virtual reality devices with students contact virtual reality companies and put in place additional student data privacy agreements that meet each school or district's state-by-state student data privacy compliance obligations and to better protect students' privacy.

How we test security

Common Sense conducted hands-on security testing of each virtual reality or augmented reality device. We test devices based on a set of expectations for how manufacturers should handle privacy, security, and other digital rights. The goal of our testing criteria is to educate consumers about a product's privacy and security practices, and to influence technology manufacturers to take these concerns into consideration when developing their products. The Privacy Program performs hands-on basic security testing of the 10 most critical security practices that parents and educators say they need to make an informed decision.[104] These security practices include actual information collection from a virtual reality or augmented reality device and any companion applications, and the transmission of information between the device and the internet.

Security framework

The following five security evaluation concern categories comprise a total of 10 critical basic security questions. These security questions illustrate the diverse security-related issues needed to complete a basic security assessment of virtual reality devices:

Data sharing

Evaluating data sharing takes into consideration best practices of keeping personal data inside the application or virtual reality device to protect privacy. Connecting social media accounts could allow people to share personal information with other people and with third-party companies. In addition, installing third-party apps with a virtual reality device could allow personal information to be collected and used for a different purpose under a different privacy policy. Criteria for data sharing include sharing with: 1) social media accounts and 2) a third-party app store.

Data safety

Evaluating data safety takes into consideration best practices of using privacy protections by default and limiting potential interactions with others. It's better to start with the maximum privacy that the app or device can provide, and then give users the choice to change the settings.[105] In addition, users talking to other people through the app or virtual reality device might permit sharing personal information with strangers. Criteria for data safety include: 3) providing privacy-protecting controls and 4) limiting social interactions.

Account protection

Evaluating account protection takes into consideration best practices of using strong passwords and providing accounts for children with parental controls. Strong passwords can help prevent unauthorized access to personal information. Children younger than 13 may not understand when they are sharing personal information, so they should be required to create special accounts with more protection under the law.[106] Lastly, parents and caregivers can help children under the age of 13 use a device or app with digital well-being protections in mind by using parental controls. Criteria for account protection include: 5) requiring a strong password, 6) displaying an age gate, and 7) providing parental controls and optional child profile.

Device security

Evaluating device security takes into consideration best practices of securing personal information against unwanted use that is shared between a mobile device, personal computer, VR device, and the internet. Keeping personal information encrypted[107], or masked[108] protects information during transmission.[109] In addition, advertising and tracking requests from the device or app could contain personal information about the user, including what they're doing with the device or app.

[104] *See* Common Sense Privacy Program, Security Testing: https://privacy.commonsense.org/resource/security-testing.

[105] *See* General Data Protection Regulation (EU) 2016/679 (GDPR) (generally, provides for data subjects to opt in); *See also* California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code § 1798.140 (generally, provides for data subjects to opt out).

[106] COPPA, 16 C.F.R. Part 312.

[107] Encryption is the process of converting messages in ordinary language, or other information, into a coded form that cannot be interpreted without knowing the secret method for interpretation, called the key, in order to prevent unauthorized access.

[108] Data masking is the process of hiding original data with modified content, used to protect data.

[109] De-encryption is the conversion of encrypted data into its original form. Reidentification is the practice of matching anonymous data with publicly available data or auxiliary data in order to discover the individual to which the data belongs to. While encryption and anonymization are not perfect, these measures provide some security over allowing unencrypted data to pass over public channels (i.e., passed from product to product via internet protocols).

Criteria for device security include: 8) securing data, and 9) observing advertising and tracking requests.

Software updates

Evaluating software updates takes into consideration best practices of keeping a device secure with up-to-date software security patches and settings. When a company improves its app or device features, better privacy and security should be part of the package and should be automatically updated or easy to update. Software and firmware updates also should be transmitted to the device in an encrypted manner to ensure a device's software cannot be intercepted and modified with malware. Criteria for software updates include: 10) updates available.

Please see the Methodology section in the Appendix for more details.

Security Results

Our hands-on security testing of the following virtual reality devices focused on the 10 most critical security practices around the collection of information from the device and on the transmission of information between the device, a personal computer, or companion mobile application, and the internet. All VR devices we tested are designed to integrate with specific software platforms that have different features for different audiences. While some devices are designed with business needs in mind, others are designed for gaming, or for a specific app ecosystem, or interoperability across platforms.

Compare security practices

Table 4 summarizes and compares the security practices of the VR devices described in each corresponding section in the remainder of this report.

- The Privacy Notices row indicates whether a privacy policy and other notices are provided during the VR device setup process. It is important that a company explain its data collection and use practices before a user puts on a VR device, not after.
- The Voice Assistant Integration row indicates whether the VR devices integrate a voice assistant, such as Siri or Google. If a VR device indicates it will be listening for any voice commands to use with a voice assistant, it is important to know so the feature can be turned on or off before use of a VR device.
- The Companion Software row indicates whether the VR device requires additional software and accounts in order to use the device. In addition to the privacy practices of each VR device, any software that is installed on a personal computer to support the VR device must also be evaluated because it could have different data collection and use practices than the headset.
- The Safety Settings row indicates whether the VR device provides safety controls for the user to determine how their profile information is displayed to others and if social interactions can be managed. Some VR apps and devices have settings you can turn on or off to make your experience safer. It's important to change these settings before you start your VR experience, not after.
- The Strong Passwords row indicates whether creation of an account to use the VR device requires a strong passphrase to protect the user's information. A requirement that the user create a strong passphrase protects the user's data from unauthorized access and demonstrates the VR device engages in reasonable security practices.
- The Children & Teens Intended row indicates whether the VR device's policies disclose children and teens are intended to use the device. It is important for parents to know whether a VR device was designed with children and teens in mind.
- The Parental Controls row indicates whether there are settings or controls on the device or companion software for parents to supervise use of the device by children. If children or teens are using a VR device, it is important that parents have settings or controls to limit use of the device based on age recommendations.
- The Child Profiles row indicates whether the VR device or companion software allow the creation of child profiles or accounts to limit inappropriate content and social interactions. If children or teens are using a VR device, they should have their own profile with stronger privacy protections and better safety settings.
- The Child Privacy Protections row indicates whether the VR device's policies disclose separate privacy protections for children and teens. If children or teens are using a VR device, the company should disclose they put in place stronger privacy protections.
- The Default Marketing Privacy row indicates whether the device manufacturer's default marketing communications options are set to opt in or the most privacy preserving best practices. The purchase and use of an expensive VR device should not require users to receive third-party marketing communications for additional products to buy.
- The Developer's Marketing row indicates whether the VR device's policies disclose the device manufacturer may send users its own first-party marketing communications. It is important for users to understand what related communications they may receive from the VR device manufacturer.

- The Third-Party Marketing row indicates whether the VR device's policies disclose the device manufacturer may send third-party marketing communications to the user for unrelated products and services. It is important for users to understand what choices they have about unrelated communications they may receive from unknown companies.
- The Default Advertising Privacy row indicates whether the device manufacturer's default advertising settings are set to opt in or the most privacy preserving best practices. The purchase and use of an expensive VR device should not require users to receive advertising that persuades them to purchase additional products.
- The First-Party Advertising row indicates whether the VR device's policies disclose the device manufacturer may display its own first-party advertising. It is important for users to understand what expected first-party advertisements they may receive from the VR device manufacturer.
- The Third-Party Advertising row indicates whether the VR device's policies disclose that the device manufacturer may display third-party advertising to the user for unrelated products and services. It is important for users to understand what choices they have about unexpected third-party advertising they may receive from unknown companies.
- The Third-Party Tracking row indicates whether observational requests were sent by the VR device to known categories of tracking activity based on the domain contacted, and as categorized by DuckDuckGo's Tracker Radar project. It is important to understand which third-party companies a VR device shares the sensitive data it collects from users.
- Lastly, the Data Encrypted row indicates whether software updates sent to the device were transmitted over the internet using standard encryption protocols. Use of encryption that protects software and firmware updates from unauthorized access demonstrates the VR device manufacturer engages in reasonable security practices.

Software platforms

Wireless virtual reality devices include the Meta Quest 2 VR device and HoloLens 2, which are standalone wireless devices that do not require the use of a personal computer or other hardware, and can install apps and content directly from their own app stores. Tethered or wired virtual reality devices require software available on various platforms that are installed on a user's personal computer to display content on the VR device.

SteamVR is a popular virtual reality software platform that is part of the Steam gaming service by Valve. The SteamVR platform uses the OpenVR SDK [110] to support interoperability with headsets from multiple manufacturers, including HTC, Windows Mixed Reality headset manufacturers, and Valve themselves. PlayStation VR, developed by Sony Computer Entertainment, is a tethered VR device for use with a PlayStation 4 or 5 console to play VR video games. Lastly, Windows Mixed Reality (also referred to as Windows MR or WMR) is developed by the Microsoft Corporation for Windows 10 PCs and includes tethered devices like the HP Reverb G2.

The *Meta Quest 2* is a self-contained VR device with access to a large catalog of games, entertainment, productivity, and fitness apps for purchase from the Meta App Store. The Quest 2 can also be connected to a user's personal computer (PC) with a wired "link cable" or wirelessly with an experimental setting called AirLink that allows users to play VR games purchased from other software platforms, such as SteamVR or the Oculus desktop app. [111] The *PlayStation VR* device is only compatible with PlayStation 4 and 5 gaming consoles and is intended to be used only with compatible VR titles purchased through the PlayStation Store. [112] The *Valve Index* device is designed to be used primarily with SteamVR which is a game store and software distribution platform for PCs. [113]

The *HP Reverb G2* device and *HTC Vive Cosmos Elite* are also designed to be compatible with SteamVR and PC VR games. The *HP Reverb G2* is unique in that it is also compatible with Microsoft's Windows Mixed Reality (WMR) software , which is a business audience focused VR portal environment to purchase and launch applications directly from a user's desktop and the Microsoft Store. [114] The *Microsoft HoloLens 2* uses a device specific version of Microsoft Windows 10 that provides access to the Mixed Reality Microsoft App Store on the device to download HoloLens specific applications that integrate with a user's Microsoft Account. The HoloLens 2 is not compatible with SteamVR, because it only uses AR specific applications from the Microsoft App Store. Lastly, the *Pimax Vision 5K* is a tethered device that connects to a personal computer and is configured by a software application called Pitool, which allows the Pimax Game Launcher inside Pitool to launch games and also connects directly with SteamVR or Oculus desktop app for content.

There are several different VR Home environments where users can create their own personalized space and access downloaded or purchased VR applications. Most VR devices can use the SteamVR Home environment, but the Meta Quest 2 uses its own Oculus Home

[110] *See* OpenVR API documentation, https://github.com/ValveSoftware/openvr/wiki/API-Documentation.
[111] *See* Meta Quest, Get Started in VR: https://www.oculus.com/setup.
[112] *See* PlayStation VR Games: https://www.playstation.com/en-us/ps-vr/ps-vr-games.
[113] *See* Steam Store: https://store.steampowered.com.
[114] *See* Microsoft Mixed Reality Portal: https://www.microsoft.com/en-us/p/mixed-reality-portal/9ng1h8b3zc7m.

Table 4: Virtual reality security categories

	Microsoft HoloLens 2	HP Reverb G2	HTC Vive Cosmos Elite	PlayStation VR	Meta Quest 2	Valve Index	Pimax Vision 5K Super
Privacy Notices	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Voice Assistant Integration	Yes	Yes	No	Yes	Yes	No	No
Companion Software	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Safety Settings	No	No	No	Yes	Yes	No	No
Strong Passwords	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Children & Teens Intended	Yes	No	No	Yes	No	Yes	No
Parental Controls	Yes	No	No	Yes	No	Yes	No
Child Profiles	No	No	No	Yes	No	Yes	No
Child Privacy Protections	No	No	No	No	No	No	No
Default Marketing Privacy	No	Yes	No	No	Yes	Yes	Yes
Developer's Marketing	Yes	No	Yes	Yes	Yes	No	No
Third-Party Marketing	Yes	No	Yes	Yes	Yes	No	No
Default Advertising Privacy	No	Yes	No	Yes	No	Yes	Yes
First-Party Advertising	No	No	Yes	Yes	Yes	Yes	No
Third-Party Advertising	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Third-Party Tracking	No	Yes	Yes	Yes	Yes	Yes	No
Data Encrypted	No	Yes	Mixed	No	Yes	Yes	Yes

Table 5: VR device software platform (Empty cells indicate the respective device does not function in the respective ecosystem)

Device	Meta App Store	Oculus Desktop	Oculus Home	Steam VR	Play Station VR	HTC Viveport Desktop	Windows Mixed Reality	Pimax PiTool
Microsoft HoloLens 2							Yes	
HP Reverb G2				Yes			Yes	
HTC Vive Cosmos Elite				Yes		Yes		
PlayStation VR					Yes			
Meta Quest 2	Yes	Yes	Yes	Yes				
Valve Index				Yes				
Pimax Vision 5K		Yes		Yes				Yes

environment, and the HP Reverb G2 and Microsoft HoloLens use variations of the Windows Mixed Reality Home environment. The HTC Vive Cosmos also has its own Viveport Home environment and PlayStation VR uses its default console environment.

Privacy notice

Every VR device should display to the user its privacy policy and any additional policies that relate to the VR device's data collection, use, or sharing practices. In addition, VR devices should also summarize the most important data privacy practices to users to help them understand the VR devices data collection practices and allow the consumer to provide informed consent. During the setup process, every VR device tested appropriately displayed its privacy policies in a conspicuous manner that allowed the user to access and view the policy before using the VR device.

Meta Quest 2 For the *Meta Quest 2*, the setup process requires consent to the Facebook Terms of Service[115], Supplemental Oculus Terms of Service, [116] Facebook Data Policy, [117] and Supplemental Oculus Data Policy. [118] In addition, if the user turns on hand-tracking gestures, they are also required to provide consent to the Hand-Tracking Privacy Notice. [119]

PlayStation VR For the *PlayStation VR*, a user must provide consent to the PlayStation 5 System Software License Agreement, [120] and is presented with notice to read the Health and Legal Information [121] during the account setup process. The user must also agree to the Terms of Service and User Agreement, [122] Privacy Policy, [123] Privacy Information for Young Players, [124] About Ratings and Parental Controls, [125] and Community Code of Conduct. [126]

Valve Index The *Valve Index* provides notice to users while installing the application Steam [127] that they must agree to Steam's Privacy Policy, [128] Terms of Use, [129] Subscriber Agreement [130], and Valve's Hardware Warranty. [131]

HP Reverb G2 The *HP Reverb G2* only requires users to provide consent to the Microsoft Privacy Policy [132] and Terms of Use [133] during setup. Interestingly, the HP

[115] *See* Facebook Terms of Service: https://www.facebook.com/legal/terms.
[116] *See* Supplemental Oculus Terms of Service: https://www.oculus.com/legal/terms-of-service.
[117] *See* Facebook Data Policy: https://www.facebook.com/privacy/explanation.
[118] *See* Supplemental Oculus Data Policy: https://www.oculus.com/legal/privacy-policy.
[119] *See* Oculus Hand Tracking Privacy Notice: https://support.oculus.com/articles/accounts/privacy-information-and-settings/hand-tracking-privacy-notice.
[120] *See* PlayStation System Software License Agreement: https://doc.dl.playstation.net/doc/ps5-eula/ps5_eula_en.html.
[121] *See* PlayStation Health Warnings: https://www.playstation.com/en-us/legal/health-warning.
[122] *See* PlayStation Terms of Service and User Agreement: https://www.playstation.com/en-us/legal/psn-terms-of-service.
[123] *See* PlayStation Privacy Policy: https://www.playstation.com/en-us/legal/privacy-policy.
[124] *See* PlayStation Privacy Information for Young Players: https://www.playstation.com/en-us/legal/privacy-information-for-young-players.
[125] *See* PlayStation About Ratings and Parental Controls: https://www.playstation.com/en-us/legal/ratings.
[126] *See* PlayStation Network Code of Conduct: https://www.playstation.com/en-us/support/account/community-code-of-conduct.
[127] *See* Steam: https://store.steampowered.com.
[128] *See* Steam Privacy Statement: https://store.steampowered.com/privacy_agreement.
[129] *See* Valve Terms of Use: https://www.valvesoftware.com/en/legal/site-terms-of-use.
[130] *See* Steam Subscriber Agreement: https://store.steampowered.com/subscriber_agreement.
[131] *See* Valve Hardware Warranty: https://help.steampowered.com/en/faqs/view/4E41-6123-79EF-25BA.
[132] *See* Microsoft Privacy Statement: https://privacy.microsoft.com/en-us/privacystatement.
[133] *See* Microsoft Terms of Use: https://www.microsoft.com/en-us/legal/terms-of-use.

Reverb G2 device did not require users to provide consent to HP's own privacy policy[134], which covers use of the device. Instead the HP Reverb G2 completely leverages Microsoft's Mixed Reality's policies to use the device.

HTC Vive Cosmos Elite The *HTC Vive Cosmos Elite* requires installation of Viveport, and during the setup process, users must agree to the Viveport Terms of Use,[135] Viveport Platform Agreement,[136] HTC EULA,[137] and HTC Terms of Use[138] as well as the HTC privacy policy.[139] In order to sign in, all users must also agree to the Account Terms and Conditions[140] and the Privacy Policy.[141] In addition, the Vive Cosmos displays a Health and Safety notice with a link to the Safety and Regulatory Guide.[142] HTC says "adults should monitor use by older children closely and avoid prolonged use." Lastly, if users purchase the optional wireless adapter, they must also agree to the Display Link EULA before downloading and installing the additional software.[143]

Microsoft HoloLens 2 The *Microsoft HoloLens 2* setup process requires users to provide consent to the Windows 10 License Agreement[144] on the device itself, and provides links to its privacy policy[145] at several different points during the device setup process. Microsoft also provides a contextual "learn more" link at different points during the setup process that allows users to jump to Microsoft's Privacy Dashboard[146] or the respective sections of its privacy policy that cover location-based services, speech recognition data, and diagnostic data. Lastly, the privacy section of the Settings app on the device displays links to learn more about Microsoft privacy settings FAQs, the privacy dashboard, and privacy statement.

Pixmax Vision 5K The *Pimax Vision 5K* setup process is the quickest and simplest of all the virtual reality devices tested. The Pimax does not require an account and is designed to be used primarily with SteamVR or Oculus desktop app. The device requires a user to download and install the Pimax Pitool configuration utility. The utility prompts the user to connect their Pimax virtual reality device, pair controllers, such as Valve's, HTC's, or Pimax's own sword controllers. Then the utility presents the user with several menu items that include Status, Settings, My games, and Help. The privacy policy is available under the Privacy subheading under the Help menu. Although the privacy policy is available for review in the Pitool application, the user is never presented with the policy during the setup process or given the ability to provide informed consent.

Data sharing

Evaluating data sharing takes into consideration best practices of keeping personal data inside the application or VR device to protect privacy. Any time personal data is available on the internet or on another device, the possibility of unauthorized sharing or breach is increased. Connecting social media accounts could allow children or students to share personal information with other people and with third-party companies. In addition, installing third-party apps with a VR device could allow the collection and use of personal information for a different purpose.

Voice Assistant Integration

Meta Quest 2 The *Meta Quest 2* allows users to opt in to allowing their voice to be used to control the VR Device under the Settings menu. Upon activation of Voice Commands, the Quest 2 provides notice to users that "your transcripts are stored to help improve Voice Commands." The notice says that to help Voice Commands better understand requests, text transcripts and related data about a user's voice interactions are stored by default. The notice also says that Meta can use machine learning and trained reviewers to process the stored transcripts and related data to make their machine learning models smarter and more accurate.

To opt out from Meta storing your voice transcripts, a user needs to click "manage settings" rather than click the blue "confirm" button and manage their voice storage options by unselecting the pre-selected blue button and clicking "confirm." This is an example of a potential "dark pattern" with a mixed opt-in and opt-out privacy setting that by design is not privacy-protective because it may confuse users as to which setting creates the desired outcome.

Additionally, hiding the option behind a default "accept" pattern encourages users to not opt out of storing their personal voice transcriptions with Meta. A dark pattern is a user interface element that can influence a person's

[134] *See* HP Privacy Statement: https://www.hp.com/us-en/privacy/privacy.html.
[135] *See* Viveport Terms of Use: https://www.htc.com/us/terms/vive/viveport-terms-of-use.
[136] *See* Viveport Platform Agreement: https://dl4.htc.com/Web_materials/Manual/Vive/Agreement/viveport_platform_agreement_(English).pdf.
[137] *See* HTC End User License Agreement and Terms of Use - HTC Vive, Software: https://dl4.htc.com/Web_materials/Manual/Vive/EULA/HTC_VIVE_CE_EULA_USA.PDF.
[138] *See* HTC Terms of Use: https://www.htc.com/us/terms/terms-of-use.
[139] *See* HTC Privacy Policy: https://www.htc.com/us/terms/privacy.
[140] *See* HTC Account Terms and Conditions: https://account.htcvive.com/legaldoc/terms-and-conditions.
[141] *See* footnote 139.
[142] *See* HTC Vive Cosmos Safety and Regulatory Guide: https://dl4.htc.com/Web_materials/Manual/Vive_Cosmos/HUS_Safety_Guide_91H03157-00M_US_B.PDF.
[143] *See* HTC DisplayLink EULA: https://dl.vive.com/EULA/DisplayLinkSWDriverEULA_EN-US.PDF.
[144] *See* Microsoft Windows 10 License Agreement: https://www.microsoft.com/en-us/Useterms/OEM/Windows/10/Useterms_OEM_Windows_10_English.htm.
[145] *See* footnote 132.
[146] *See* Microsoft Privacy Dashboard: https://account.microsoft.com/account/privacy.

Table 6: VR device voice assistant integration

Device	Voice Assistant	Default Setting	Command	Voice Data Storage
Microsoft HoloLens 2	Yes	Opt-out	"Hey Cortana"	Opt-in
HP Reverb G2	Yes	Opt-in	"Hey Cortana"	Opt-in
HTC Vive Cosmos Elite	No	N/A	N/A	N/A
PlayStation VR	Yes	Opt-in	"Hey PlayStation"	Opt-out
Meta Quest 2	Yes	Opt-in	"Hey Facebook"	Opt-out
Valve Index	No	N/A	N/A	N/A
Pimax Vision 5K	No	N/A	N/A	N/A

behavior against their intentions or best interests.[147] However, a user can also change their voice storage preferences at any time in the Settings menu, under Voice Commands and Voice Storage.

PlayStation VR The *PlayStation VR* device allows users to opt in to enable Voice Command (Preview) which uses a user's voice to find and open games, control media, search and use available in-game voice commands. PlayStation provides notice to users that when they enable Voice Command, voice data and interactions will be collected and processed exclusively for operation, analysis, and improvement, which may include review of written transcripts by human reviewers, unless a user provides opt-out consent under the Settings menu, Users and Accounts, Privacy, and Voice Data Collection. The user must select the "don't allow" option in order to not use their voice data to improve voice features. PlayStation provides notice that "even if users don't allow us to collect your voice data, voice features won't be disabled." In addition, the option Participate in our Feedback Program is pre-selected, meaning users are required to opt out of being contacted by PlayStation to share their experiences after enabling the Voice Command option.

Valve, HTC, Pimax, and HP The *Valve Index*, *HTC Vive Cosmos Elite*, and *Pimax Vision 5K* do not integrate a voice assistant into the VR experience using their respective devices. However, users who wish to integrate voice commands in their VR experiences can download third-party desktop applications such as VoiceAttack to control their games or applications while using VR.[148] The *HP Reverb G2* allows users to opt in to use speech in mixed reality with Cortana[149] and displays a link to the Microsoft Privacy Policy for more information. The use of audio and speech in mixed reality is controlled by a setting on a user's personal computer in the Microsoft Windows control panel. The control panel provides a Mixed Reality icon and setting with a section labeled "speech recognition." The option says "Use speech recognition in Windows Mixed Reality including dictation and interacting with apps using voice commands. Speech recognition will always be listening when mixed reality is in use." Users should be aware that if the HP Reverb G2 headset is in use, and the additional opt-in "online speech recognition" setting is enabled, then everything a user says will be sent to Microsoft's cloud-based speech recognition service.

Microsoft HoloLens 2 The *Microsoft HoloLens 2* integrates with Cortana and during the device setup process the HoloLens 2 prompts users to "do more with your voice." The user is presented with the "opt out" choice to "use speech" with their HoloLens device. The notice says, "Use your voice for commands, dictation, and app interactions. When your HoloLens is on, it's always listening for your voice input and sending your voice data to Microsoft's speech service." In addition, in the Settings app on the device in the Speech section are more privacy settings for a user's voice or speech recognition data. The HoloLens displays this prominent notice to users: "Use your voice to talk to HoloLens. Your HoloLens will always be listening for your voice input when this device is on and your voice commands can be used to control your device. If you turn off speech recognition, you won't be able to use your voice for dictation or interacting with Cortana and other apps. And your HoloLens won't respond to any voice commands."

The HoloLens also provides a second voice data setting for "online speech recognition" which is opt in to "use your voice for apps using Microsoft's online speech recognition technology." Lastly, the user has a third opt-in choice to contribute their "voice clips," which may be reviewed by Microsoft employees and vendors to improve Microsoft's speech technology. Microsoft provides further notice that a user's identity is protected and "voice clips" are not linked to a user. Microsoft claims

[147] Gunawan, J., Pradeep, A., Choffnes, D., Hartzog, W., and Wilson, C. (October 2021). A comparative study of dark patterns across mobile and web modalities. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 377. https://doi.org/10.1145/3479521.

[148] *See* VoiceAttack: https://www.voiceattack.com/Default.aspx.

[149] *See* Microsoft Cortana: https://www.microsoft.com/en-us/cortana.

if they find a clip with personal information, they will delete it.

Companion applications and software

The following VR companion software is used to support each VR device, or may be optional for the user to control settings. Companion software can be a separate desktop, console, or mobile application that can have different data collection, use, and sharing practices than the VR device. VR companion software has been categorized into several types including software: installed on the user's personal computer, installed on a user's mobile device to control settings, accessible from the VR device, used primarily for social networking, or messaging that also supports VR integration.

Meta Quest 2 The *Meta Quest 2* device provides users with the option to connect their existing Facebook account, or they can create an account with Facebook online or through the mobile app, which allows them to connect with friends and family and meet new people in their social media network. Users can optionally choose to download the Oculus mobile app on their smartphone, then wirelessly connect their Quest 2 headset and phone to complete the VR device setup process. The mobile app allows users to shop VR titles from the mobile app and includes additional features, such as "casting" a user's virtual reality session of what they see in VR to the mobile phone or compatible TV set. [150] The app also allows users to find friends in VR and share experiences together, and manage their Oculus device, account, and notifications. Lastly, Quest 2 users are not required, but encouraged to use a Facebook account for messaging friends on Facebook and through VR with the Messenger app by Facebook.

PlayStation & Valve The *PlayStation VR* experience is primarily accessed through the PlayStation game console, but users can also download a mobile application called the PlayStation app, which allows users to manage their PlayStation Network account and control their game console, see which friends are online, send messages, and discover discounts for games on the PlayStation Store. The *Valve Index* requires users to download the Steam desktop application to their personal computer, which is one of the most popular online game platforms for playing, discussing, and creating games. Steam desktop comes with SteamVR, which is a software tool for experiencing VR content on various virtual reality hardware devices. SteamVR supports the *Valve Index*, *HTC Vive Cosmos*, *Meta Quest 2*, Windows Mixed Reality headsets, and others. [151] Steam also provides an optional Steam mobile application to control settings, and Steam Chat to engage in social networking activities.

HP Reverb G2 The *HP Reverb G2* utilizes SteamVR Desktop to launch the VR device and integrates all of SteamVR's settings in VR, but also launches the Windows Mixed Reality Portal support software to access VR mixed reality applications from the Microsoft Store, which can be interacted with in VR through a user's computer "desktop view". The device also requests the user install OpenXR, which is an open royalty-free API providing native access to a range of devices across the mixed reality spectrum. [152] The *HTC Vive Cosmos Elite* requires users to download a setup application to support the HTC device that installs Vive Software and the Viveport desktop app on the users' personal computer. After installation is complete, the user must create an account with Viveport and has the option of signing into Viveport with a single-sign login using their Google, Facebook, or Steam account. After login, users are prompted to join Infinity, which is HTC Vive's app store subscription service at $12.99 per month, billed monthly, or $8.99 a month with an annual subscription. Users can also choose the "maybe later" link to not join the Infinity service and continue loading the Viveport application.

In addition, there is an Infinity Lite user account that enables users to browse and make purchases from the Viveport store and access a selection of curated free VR titles. The Viveport app integrates with the *HTC Vive Cosmos Elite* device and with other non-HTC VR devices such as Windows Mixed Reality devices like the *HP Reverb G2*, or the *Valve Index*, or *Meta Quest 2* with link cable. After a user has configured their VR device, they can load the Viveport VR interactive experience or browse the Viveport store desktop app. The *HTC Vive Cosmos* device also integrates with SteamVR and loads a user's SteamVR settings and VR purchases from Steam into Viveport. The Viveport desktop application also allows a user to set up a new VR device and installs *HTC Vive Cosmos Elite* device software, which is controlled through an application called Vive Console. Users can also install the optional wireless adapter and remove the tethered link cable. [153] The wireless adapter requires additional software to be installed called Vive Wireless.

Microsoft & Pimax The *Microsoft HoloLens 2* requires users to have a Microsoft account and uses Microsoft Windows's Mixed Reality application to access the Microsoft App Store and download free or paid HoloLens specific third-party applications. These apps allow the HoloLens to be used for real-time collaboration, manipulation of 3D objects, or with industry-specific applications in manufacturing, architecture, or medicine. Lastly, the *Pimax Vision 5K* requires installation of a software

[150] Google Play Store Oculus App: https://play.google.com/store/apps/details?id=com.oculus.twilight; Apple iOS App Store: https://apps.apple.com/us/app/oculus-vr/id1366478176.

[151] *See* SteamVR: https://www.steamvr.com/en.

[152] *See* Microsoft OpenXR: https://docs.microsoft.com/en-us/windows/mixed-reality/develop/native/openxr.

[153] *See* HTC Wireless Adapter: https://www.vive.com/us/accessory/wireless-adapter.

Table 7: VR companion apps (Empty cells reflect that no apps in the respective category are explicitly bundled with a given device)

Device	Personal Computer App	Mobile Settings App	VR Device App	Social Network App	Messaging App
Microsoft HoloLens			Microsoft App Store[a]		
HP Reverb G2	Windows Mixed Reality Portal[b]				
HTC Vive Cosmos	Viveport[c], Vive Software, Console, and Wireless[d]				
PlayStation VR				PlayStation App[e]	
Meta Quest 2	Oculus[f]	Oculus[g]	Meta App Store[h]	Facebook[i]	Messenger[j]
Valve Index	SteamVR Desktop[k]	Steam[l]		Steam Chat[m]	
Pimax Vision 5K	Pitool[n]				

[a] *See* Microsoft Store, https://apps.microsoft.com/store/apps.
[b] *See* Windows Mixed Reality Launcher, https://store.steampowered.com/app/719950/Windows_Mixed_Reality_for_SteamVR.
[c] *See* Viveport, https://www.viveport.com.
[d] *See* HTC Wireless Adapter Set-up, https://www.vive.com/us/setup/wireless.
[e] *See* Google Play Store, PlayStation App, https://play.google.com/store/apps/details?id=com.scee.psxandroid&gl=US; *See also* Apple App Store, PlayStation App, https://apps.apple.com/us/app/playstation-app/id410896080.
[f] *See* Oculus Setup, https://store.facebook.com/quest/setup.
[g] *See* Apple App Store, Oculus, https://apps.apple.com/us/app/oculus/id1366478176; Google Play Store, Oculus, https://play.google.com/store/apps/details?id=com.oculus.twilight&gl=US.
[h] *See* Meta Quest Store, https://www.oculus.com/experiences/quest.
[i] *See* Apple App Store, Facebook, https://apps.apple.com/us/app/facebook/id284882215; Google Play Store, Facebook, https://play.google.com/store/apps/details?id=com.facebook.katana&gl=US.
[j] *See* Messenger, https://apps.apple.com/us/app/messenger/id454638411; Google Play Store, Messenger, https://play.google.com/store/apps/details?id=com.facebook.orca&gl=US.
[l] *See* Steam, Google Play Store, https://play.google.com/store/apps/details?id=com.valvesoftware.android.steam.community&gl=US.
[m] *See* Steam Chat, Google Play Store, https://play.google.com/store/apps/details?id=com.valvesoftware.android.steam.friendsui.
[n] *See* Pimax Pitool, https://pimax.com/pitool-download.
[k] *See* Steam, https://store.steampowered.com.

application on a personal computer called Pitool, which is a simple utility to determine the status of the device and configure its settings. The Pimax device integrates with other VR software distribution platforms for content.

Most of the privacy policies of the virtual reality devices tested in this report also cover the use of additional personal computer software or mobile applications required to use the device. However, sometimes the companion software or mobile applications have different privacy policies than the same company's virtual reality device. The *Meta Quest 2* device includes the companion apps *Facebook* and *Messenger*, which have different privacy policies than the Quest 2, but both receive about the same overall score and have the same "worse" privacy rating practices as Oculus.

The *Meta*, *Facebook*, *Messenger*, *PlayStation app*, and *Microsoft* privacy policies all claim they do not sell a user's data to third parties, which is initially promising because it is a better privacy-protecting practice. Only *HTC* was explicitly clear in their privacy policy that they sell users' data to third parties for profit. However, our privacy evaluations of the most popular virtual reality companion applications indicate that all devices have privacy practices that put consumers' privacy at considerable risk.

Almost all of the virtual reality companion applications state in their privacy policies that they can use a user's sensitive data collected in virtual reality for commercial purposes that include selling their data to third parties, sending third-party marketing communications, displaying targeted advertisements, tracking users across other sites and services, and creating advertising profiles for data brokers. Lastly, the *Steam* privacy policy is nontransparent or unclear on all of our privacy rating criteria, which means there can be no future expectation of what data is collected by the device or how it can be used or shared with third parties.

User safety

Evaluating data safety in the context of data privacy takes into consideration best practices of using privacy protections by default and limiting potential social interactions with others. It's better to start with the maximum privacy that the app or device can provide, and then give users the choice to change the settings. It's also better to have people opt in to sharing rather than forcing them to opt out if they want to protect their privacy. In addition, users talking to other people through the app or device might permit personal information to be shared with strangers or be made publicly available.

The SteamVR companion app provides an integrated Friends and Chat application through the Steam desktop application with friends that can be added or removed by a username.[154] The chat application can be used within the Steam application or through a web browser or the mobile app.[155] However, a user's Steam account profile does not provide any safety-related controls beyond blocking users and filtering specific chat words. Unfortunately, the *Valve*, *HP*, *HTC*, and *Pimax* VR devices that use SteamVR do not provide any additional safety settings which can put kids and families at risk for privacy and safety harms.

The *Meta Quest 2* and the *PlayStation VR* are the only VR devices we tested that integrate social interactions with other users through their companion software with safety controls. Therefore, the following analysis looks at only these two VR devices and their safety controls or settings with a focus on privacy by design and the safest option for kids and families.

Meta Quest 2

The Meta Quest 2 device itself does not provide any privacy settings related to changing how a user's personal information can be used by Meta or third parties for advertising, tracking, ad profiling or third-party marketing communications. However, the Meta account webpage does provide additional privacy settings for users not available on the VR device, such as email preferences.[156] The Meta website does provide users with a Safety Center website with resources on how to keep users safe in VR.[157]

The Quest 2 device does provide users with safety settings that relate to how other users will see their activity, friends list, or name while using the device. In addition, a user's privacy settings are also inherited from their Facebook account privacy settings. It is recommended that a user also review their separate Facebook privacy account settings through the Facebook application or in a web browser online before use of the Quest 2 device.[158]

The Oculus desktop application installed on a user's personal computer also has the same settings as the Quest 2 device under Settings, then Privacy. Lastly, Meta has recently announced new Meta accounts that will allow users to control what people can see when they view a user's Meta Horizon profile. This new account will introduce three privacy options: Open to Everyone, Friends and Family, and Solo. Meta says that new Meta account users between ages 13 and 17 will have their Meta

[154] *See* Steam, Steam Friends & Chat: https://help.steampowered.com/en/faqs/view/595C-42F4-3B66-E02F.
[155] *See* the All-New Steam Chat: https://steamcommunity.com/updates/chatupdate.
[156] *See* Meta Quest, Account Details: https://secure.oculus.com/my/emails.
[157] *See* Meta, Safety Center: https://www.oculus.com/safety-center.
[158] *See* Facebook Privacy Basics: https://www.facebook.com/about/basics/manage-your-privacy.

Table 8: Privacy ratings of companion apps

App	Privacy Rating	Sell Data	Third-Party Marketing	Targeted Ads	Third-Party Tracking	Track Users	Ad Profile
Microsoft App Store[a]	75% Warning	No	Yes	Yes	Yes	Yes	Yes
Windows Mixed Reality Portal[b]	72% Warning	No	Yes	Yes	Yes	Yes	Yes
HTC Viveport[c]	51% Warning	Yes	Yes	Yes	Yes	Yes	Yes
PlayStation App[d]	50% Warning	No	Yes	Yes	Yes	Yes	Unclear
Facebook[e]	49% Warning	No	Yes	Yes	Yes	Yes	Yes
Messenger[f]	49% Warning	No	Yes	Yes	Yes	Yes	Yes
Oculus[g]	48% Warning	Unclear	Yes	Yes	Yes	Yes	Yes
SteamVR Desktop[h]	44% Warning	Unclear	Unclear	Unclear	Unclear	Unclear	Unclear
Pimax Pitool[i]	30% Warning	Unclear	Yes	Yes	Unclear	Unclear	Unclear

[a] The Microsoft App Store is available within the HoloLens experience. *See* Common Sense Privacy Evaluation for HoloLens, https://privacy.commonsense.org/evaluation/Microsoft-Hololens.
[b] *See* Common Sense Privacy Evaluation for Microsoft Mixed Reality, https://privacy.commonsense.org/evaluation/Microsoft-Mixed-Reality.
[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 Facebook, https://privacy.commonsense.org/evaluation/Facebook.
[f] *See* Common Sense Privacy Evaluation for Messenger, https://privacy.commonsense.org/evaluation/Messenger.
[g] *See* Common Sense Privacy Evaluation for Oculus, https://privacy.commonsense.org/evaluation/Oculus.
[h] *See* Common Sense Privacy Evaluation for Steam, https://privacy.commonsense.org/evaluation/Steam.
[i] *See* Common Sense Privacy Evaluation for Pimax, https://privacy.commonsense.org/evaluation/Pimax.

Horizon profiles set to Solo by default, which means it is the most privacy-protecting setting.[159]

The following settings are available in the Oculus desktop application and within the Quest 2 VR experience:

Activity The Activity setting controls who will see a user's activity on Oculus. A user's presence in specific apps may be visible to others if they participate in social activities like parties, events, or leaderboards.

Table 9: Activity setting on Meta Quest 2

Option	Safest Choice
Public	No
Friends on Oculus	No
Only me	Yes

It is important for users and parents and caregivers to set appropriate boundaries in virtual reality environments, and that includes limiting who can interact with a user in VR in order to decrease the risk of potential social or emotional harm. In real life, only other people in the same physical location who are in close proximity to an individual are aware directly, or indirectly, of that individual's activity in the party or event. However, this can also include inferring a user's real-life activity from digital footprints, like their online status, to location through the use of GPS tracking devices, use of third-party apps, or other patterns that could indicate a user's real-life routines or activity. This could include people an individual knows in real life, like friends or family, or even other unknown members of the public, like at a sporting event. Therefore, just like in real life, it is important to set similar boundaries in virtual reality environments and with our digital footprints to only let people a user knows in real life be notified when they are using their virtual reality device because there is shared mutual trust.

However, Meta's all-or-nothing Friends on Oculus setting may not be the safest choice because if a user has made lots of "friends" on Facebook that they have never met in real life, it may not be appropriate to let all those users know your private activity at all times when using a Meta Quest device. The most privacy-protecting option is to choose Only Me, so a user has complete control over which individuals have access to see their activity on the device, just like in real life. And if a user feels comfortable with this privacy setting, then they can expand it to include other friends upon request.

Friends list The friends list setting controls who can see a user's friend list on Oculus. A user can control who can see who their friends are on Oculus. In addition, mutual friends will always be visible, and apps a user owns

[159] *See* Introducing Meta Accounts and Meta Horizon Profiles for VR: https://about.fb.com/news/2022/07/meta-accounts-and-horizon-profiles-for-vr.

can see their friends who own the same app, so they can easily compare high scores and interact with each other.

Table 10: Friends list setting on Meta Quest 2

Option	Safest Choice
Public	No
Friends on Oculus	No
Only me	Yes

Friends lists are often considered private because they are really a social network or collection of who you know and have decided to trust. However, most Facebook users would say they have more Facebook friends than contacts in their cellphone because shared trust is different with people who may have met online and people you know in real life. As previously discussed, Meta's all-or-nothing Friends on Oculus setting may not be the safest choice because if a user has made lots of "friends" on Facebook that they have never met in real life, then there is no mutual trust and it may not be appropriate to let other players or friends you have just met know who all your friends are when using a Meta Quest device. The most privacy-protecting option is to choose Only Me, so a user has complete control over which individuals have access to see their activity on the device, just like in real life. And if a user feels comfortable with this privacy setting, then they can expand it to include other friends upon request.

Facebook name The Facebook name setting controls who will see a user's Facebook name on Oculus.

Table 11: Facebook name setting on Meta Quest 2

Option	Safest Choice
Public	No
Facebook Friends on Oculus	No
Only me	Yes

When it comes to sharing your real name or identity with other users on Oculus, it's important to follow the rules that would also apply in real life. Parents and caregivers should be aware that users should not share their real name with strangers, but only trusted individuals who know their identity in real life. If a user does not feel comfortable sharing their real name with all their Facebook friends, Meta allows users to choose a nickname or screen name through the Oculus website to be displayed to their Facebook Friends and other users rather than a user's real name. [160]

Similarly, Meta's all-or-nothing Facebook Friends on Oculus setting may not be the safest choice because if a user has made lots of "friends" on Facebook that they have never met in real life, then there may be no shared mutual trust and it may not be appropriate to let other players or friends you have just met know your Facebook name. The most privacy-protecting option is to choose Only Me, so a user has complete control over which individuals have access to see their activity on the device, just like in real life. And if a user feels comfortable with this privacy setting, then they can expand it to include other friends upon request.

Active status push notifications Who can receive push notifications to know when you're active in VR and your activity? You can choose who sees a push notification from the Oculus mobile app about your active status and what apps you're using.

Table 12: Active status setting on Meta Quest 2

Option	Safest Choice
Facebook Friends on Oculus	No
Only me	Yes

Push notifications that pop up and interrupt users to let them know a friend is online can be a great feature for staying connected with close friends who want to connect and experience virtual reality together. However, as previously discussed Meta's all-or-nothing Facebook Friends on Oculus setting may not be the safest choice because if a user has made lots of "friends" on Facebook that they have never met in real life, then there may be no shared mutual trust and it may not be appropriate to let other friends you have just met know you are actively using your VR device.

Users may not want to unfriend other users to avoid them knowing their active status in VR. Also this notification tool could also be abused if friends a user has made on Facebook know a user's active online status and may send unwanted communication messages. The most privacy-protecting option is to choose Only Me, so a user has complete control over which individuals have access to see their activity on the device, just like in real life. And if a user feels comfortable with this privacy setting, then they can expand it to include all their Facebook friends.

Blocked users Similar to blocking unwanted phone numbers or senders of text messages on your mobile device, the Meta Quest 2 settings provide the ability for users or their parents or caregivers to block specific Oculus user accounts from communicating with them to avoid potential cyberbullying, cyberstalking, or harassment. This social communication blocking feature is especially important in virtual reality where harassment or unwanted social interactions between users can include visual, audio, gestural, and written chat communications. Without blocking features, users may not be able to avoid interacting with VR content and activity before harm has occurred especially for known repeat

[160] *See* Meta, Log In with Facebook: https://auth.oculus.com/login.

Table 13: PlayStation VR privacy settings

	Default Setting	Option Setting	Privacy Protective Setting
Data You Provide	Enabled "Full"	Opt-out	"Limited"
Personalized Purchase Recommendations	Enabled	Opt-out	Not Enabled
Personalized Advertising	Enabled	Opt-out	Not Enabled
Personalized Media	Enabled	Opt-out	Not Enabled

offenders: A disturbing image may appear suddenly, inappropriate gestures may happen without warning, disturbing comments may be heard before a device or user can be muted, abusive chat communications may be seen before users can be blocked, and finally notifications that pop up and appear in front of a user may not be possible to avoid seeing.

PlayStation VR

The PlayStation VR device by default enables a privacy setting called Data You Provide under the Settings → Users and Accounts → Privacy submenu which says "*to improve our services, we retain certain usage data. Choose how much you're comfortable sharing. Your data will always be protected.*" Users are required to opt out from Full information sharing with PlayStation that includes detailed information about a user's network connection, device, and video streams. PlayStation does provide a helpful notice to users to support informed consent about what is Device Data, which includes behavioral data such as *"more detailed information about you such as what you click on in a menu, pages you have viewed, or how far you got in a game."*

A user must select the Limited option to share only necessary data with PlayStation to maintain and operate core PlayStation features and services. This is an example of a privacy setting that by design is not privacy-protective because by default the device shares more information than is necessary to provide the user with the features and game experience they requested. This practice can increase risk because PlayStation's privacy policy says depending on your settings device data may be used to *"deliver target and personalize advertising, commercial recommendations and marketing communications."*

In addition, the color of the slider selection toggle is the color gray when selected. Most other interfaces indicate a color change to green or blue if the setting toggle is enabled. It was difficult to determine whether the single toggle had been selected during testing. However, when one option toggle is selected and another option toggle is not selected below, it is easier in this situation to determine the status of whether the option is enabled or disabled. If more than one setting toggle is selected without any color except gray, then it is not easy for a user to determine whether the setting is enabled or disabled, which could be considered a dark pattern. [161]

Under the Personalization menu, users have the option to opt in or opt out of several advertising and recommendation related privacy settings. "*Personalized Purchase Recommendations*" is disabled by default, and users can opt in to allow the PlayStation Store "to show you personalized product and service recommendations (sometimes assisted by data from third-party sources). When disabled, you'll still see offers and recommendations, but they may be less relevant." This setting allows PlayStation to customize advertising in its own store, based on tracking your behavioral data while using the gaming console or VR device.

The "*Personalized Media*" option, which is enabled by default, allows PlayStation to display *"personalized video and music recommendations from integrated media providers and apps. When disabled, you still might see recommendations directly from partner media services."* Again, PlayStation is trying to customize advertising through video and music content in its own store, based on tracking your behavioral data while using the gaming console or VR device. This type of personalized media engagement is likely a precursor to targeted advertisements because the practice is aimed at increasing the amount of time and interactions users have on the PlayStation device to maximize advertising and tracking data collection. Lastly, the "*Standard Personalization*" option which is enabled by default allows PlayStation *"to show you general noncommercial personalization. If disabled, some features will still be personalized but they will be less relevant."* This last option is more about relevant profile and game feature personalization that does not include commercial purposes and should be safe for use. PlayStation does provide a helpful notice to users at the point of their decision about these personalization options to view their privacy policy for more information.

Additionally, and as seen in Table 14, users can select Adjust Privacy Settings by Choosing a Profile, which is a helpful way for users who are unsure about which settings to change to better protect their privacy and safety.

[161] *See* footnote 147.

Table 14: PlayStation VR choosing a profile

Profile	Description	Privacy Protective Setting
Social and Open	I like to maximize my chances to connect, be seen, and socialize	Not Enabled
Team Player	Effortless multiplayer, but I limit who knows my real identity	Not Enabled
Friend Focused	Anything for my crew, more restrictive for strangers	Not Enabled
Solo and Focused	I keep a low profile, and choose who I interact with	Enabled

It is recommended that users start with the most privacy- and safety-protecting setting of Solo and Focused to better understand what social interactions are available or disabled, and what information is visible to other users. As users become more comfortable with their understanding of PlayStation's safety controls and interactions with friends and strangers, they can move to the next Friend Focused option if they want additional interaction features. Lastly, users can "review and customize" any of the preset profiles to mix and match specific safety settings to create customized profiles that exist between the default profile options. PlayStation's safety settings are considered best privacy-by-design settings that enable users to make informed decisions about their data and remain in control of their social interactions with friends and other users in order to minimize potential harm.

PlayStation users can also use View and Customize Your Privacy Settings for each of the specific options, rather than choosing a quick default profile or customizing a preset profile. The following PlayStation privacy options are provided to users to select based on social-networking principles of trust of close friends you likely know in real life, and indirect friends of friends you do not know in real life but may like to meet. As discussed, the most privacy-protecting settings are to not share real names or pictures of yourself, or your friends, with strangers or users you don't trust. It is important for users to create a privacy and safety profile that reflects as closely as possible their real world preferences regarding how they interact with friends and strangers, what personal information they share about themselves with others, and who can see them.

Table 15: PlayStation VR customize privacy settings: Your real name and profile picture

Setting	Options	Privacy Protective Setting
Who can see them in search results	No One/Anyone	No One
Who can see them within games	Close Friends/No One	No One
Who can see them as a friend suggestion	No One/Close Friends of Friends	No One
Who can see them in your close friends' list of friends	Close Friends of Friends/Close Friends Only	Close Friends

When it comes to letting other people see who a user's friends are, it's important to keep in mind their friends' expectations and behavior regarding privacy. Would someone be OK with their friends in real life telling other people that they do not know details about their name or usernames or about their online relationship? Would it matter if a user's friends are under 18 and people who they share their friends' names with are over 18, or male or female? The most privacy protective setting is No One, so a user's friends' information is not shared with anyone they do not know. However, if multiple friends already know each other it may be better to choose Friends Only, so only people a user trusts can see each other and help make new friendships based on already existing relationships.

Table 16: PlayStation VR customize privacy settings: Your information

Setting	Options	Privacy Protective Setting
Who can see your friends	No One/Friends Only/Friends of Friends, Anyone	No One
Edit Your Profile	Change one or more characteristics	N/A

Users may not want anyone knowing they are online and what games they have been playing. Having access to this information could allow people, including people

they do not know, to track their activity, much like tracking where a user goes or what they do in real life. Sharing this information could even lead to problematic behaviors, such as cyberstalking or harassment. Letting trusted users know when they are online allows friends to know when the user is available and if friends can contact them to join them in a game. However, a user's gaming history of what games they played, for how long they played, and when they played them, may be too much information for a user to share with all their friends or with strangers. Therefore, when it comes to sharing a user's activity information over time it is recommended to choose the most privacy protecting setting of No One, especially for younger users.

Table 17: PlayStation VR customize privacy settings: Your activity

Setting	Options	Privacy Protective Setting
Who can see your online status and what you;re currently playing	Friends Only/Friends of Friends/Anyone	Friends Only
Who can see your gaming history	No One/Friends Only/Friends of Friends/Anyone	No One
Hide your games from other players	Choose one or more games	N/A

Before sending or accepting friend requests, which can give privileged access to more information about oneself, it's good to establish that the other potential friend is trustworthy. In real life, friends typically exchange names, friends they may have in common, shared interests, and a mobile number or other contact information to stay in touch. In the online world, it's more difficult to build trust with strangers that you do not know because they may not be telling you the truth about their age, gender, interests, or location. Even their avatar and voice may be changed[162] to hide their true identity. Therefore, it is recommended to start with the most privacy-protecting setting of No One. Then after a user feels more comfortable interacting and meeting strangers and has developed the necessary skills to assess trust in an online or VR setting such as while playing games, choosing Friends of Friends may be more beneficial to meet new people that have a shared mutual friend which can help establish and build trust.

In addition, even though a user may have made friends while playing various online games, it's also important to set appropriate boundaries of who can interact with that user through different games and messages. It is a better privacy-protecting practice to allow No One to be able to interact with a user until they initiate the conversation, much like how we interact socially in the real world. In real life, when a user receives a phone call or text message from a friend they know, they have control over whether to answer the phone call or messages. In the online world, after a user feels comfortable and trusts the friends they have made online, then choosing Friends Only will allow your friends to initiate conversation with you to join a party or game, just like receiving a phone call.

Lastly, online harassment is unfortunately commonplace, and cyberbullying, cyberstalking and other forms of harassment can happen to anyone and can even be perpetrated by users in their friends list.[163] If at any time a user feels harassed or threatened in any way, they can always choose to block a user that is their friend, or maybe a user that is not their friend, but a friend of friends. This puts users back in control by blocking and preventing future communications which may create the opportunity for harassment from other players; this is similar to blocking a phone number on their mobile device.

Table 18: PlayStation VR customize privacy settings: Communications and multiplayer

Setting	Options	Privacy Protective Setting
Who can ask to be your friend	No One/Friends of Friends/Anyone	No One
Who can interact with you through parties, games, and messages	No One/Friends Only/Anyone	No One
Players you are blocking	Choose one or more blocked players	N/A

Account protection

Evaluating account protection takes into consideration best practices of using strong passwords and providing accounts for children with parental controls. Strong passwords can prevent unauthorized access to personal

[162] *See* Voicemod: https://www.voicemod.net; *See also* Voicemod Privacy Policy: https://www.voicemod.net/privacy.

[163] ADL. (2022, May 3). *Hate is no game: Harassment and positive social experiences in online games 2021.* https://www.adl.org/resources/report/hate-no-game-harassment-and-positive-social-experiences-online-games-2021

information. Children younger than 13 may not understand when they are sharing personal information, so they should be required to create special accounts with more protection under the law. Lastly, parents and caregivers can help children younger than 13 use a device or app with digital well-being protections in mind by using parental controls.

Table 19: Strong passwords are required for accounts

Device	Strong Passwords	Account Type
Microsoft HoloLens	Yes	Microsoft
HP Reverb G2	Yes	Microsoft
HTC Vive Cosmos Elite	Yes	Viveport
PlayStation VR	Yes	PlayStation
Meta Quest 2	Yes	Facebook/Meta
Valve Index	Yes	Steam
Pimax Vision 5K	N/A	N/A

Meta Quest 2

The *Meta Quest 2* device requires users to already have a Facebook account or they can create a new account on Facebook online, or through the Facebook mobile application, which allows them to connect with friends and family and meet new people in their social media network. However, Meta recently announced that in August 2022, users can create Meta accounts to use their Quest 2 device that will allow users to log in to their VR headsets that don't require a Facebook account. In addition, once users create a Meta account, they will also need to create a Meta Horizon profile, which will be their social profile in VR. [164]

PlayStation VR

The *PlayStation VR* setup process can be completed on the console device itself connected to a television, using the provided controller, on a website on another device with a QR code, [165] or through the PlayStation App on a mobile device. [166] PlayStation requires the creation of a primary adult account. If a birthdate selected identifies someone as younger than 13, the setup process blocks the creation of a primary child account and blocks the user from changing the birthdate to reflect an age older than 13. In addition, PlayStation notifies the underage user to "hand the controller to a parent" to complete registration of their own adult account and child profile. After rebooting, an adult account can be created, which requires use of a strong password and first name, last name, and screen name, which are not visible to other players by default.

In addition, the account requires the collection of the postal code, city, and state, but a privacy notice indicates the information will only be used by PlaySation and will not be shared with others. PlayStation provides parents with tips to prevent unauthorized game purchases, such as requiring a passcode to purchase products from the PlayStation Store, or removing the credit card on file with the primary account, which must be entered each time a purchase is made.

HP & HTC

The *HP Reverb G2* does not require the user to create an account during the setup process, but does require a Microsoft Windows account to purchase apps in the Mixed Reality Windows App Store. The *HTC Vive Cosmos* setup process requests that users create a new HTC Viveport account or sign in with their Google, Facebook, or Steam account. The HTC account creation process does not require a user to provide a birthdate but does require the user to verify the email address they used during registration.

Microsoft HoloLens 2

The *HoloLens 2* initially asks users *"who owns this HoloLens? If this HoloLens belongs to your work or school, we'll set it up as theirs and you'll get access to their stuff. If you own it, we'll set it up using your Microsoft Account."* The user is then prompted to log in or create a Microsoft account to use the device.

For testing purposes, we only selected the device to be used for "work," but the "school" option could include additional features that were not explored. After the user is logged into the device with their Microsoft account, the user is presented with an opt-in choice to log on automatically to the device using an "iris" scan of their eyes. Microsoft displays a notice to the user that says, "Say goodbye to having to use passwords. Windows Iris Sign-in is a fast and secure way to sign in to your HoloLens. This data is only used for this device." In addition, a user must create a Personal Identification Number (PIN) to access their account which must be six digits long.

Pimax Vision 5K

The *Pimax Vision 5K* does not require an account to use and configure the device through the Pimax Pitool utility. However, a user will need to have a Steam account to access their content library in SteamVR or Facebook account to access their content in the Oculus desktop app.

Parental consent

For children age 13 or younger, a parent or guardian's verifiable consent is required before the collection, use,

[164] *See* footnote 159.

[165] *See* Sony Set-Up on Web: https://www.playstation.com/ps5/setuponweb.

[166] *See* iOS Apple App Store, PlayStation App: https://apps.apple.com/app/apple-store/id410896080; Google Play Store, PlayStation App: https://play.google.com/store/apps/details?id=com.scee.psxandroid.

or disclosure of the child's personal information to an application or service.[167] In addition, if children are using the application or device, then parents should be provided with controls to protect their child's personal information through child profile management or other forms of age gating or verification of age.[168]

Table 20: Parental controls are available

Device	Parental Controls	Child Profile Management
Microsoft HoloLens 2	No	No
HP Reverb G2	No	No
HTC Vive Cosmos Elite	No	No
PlayStation VR	Yes	Family Management
Meta Quest 2	Yes	Oculus Parent Hub
Valve Index	Yes	Steam Family View
Pimax Vision 5K	No	No

Only the *Microsoft HoloLens 2*, *PlayStation VR*, and *Valve Index* indicate in their privacy policies that users under the age of 13 may use their services, which means we would expect these companies to also disclose they provide parental controls. In addition, *Meta*, *PlayStation*, *Valve*, and *Microsoft* indicate users older than 13 may use their services which means parental controls would also likely be available to teens as well. However, only *Meta*, *PlayStation*, and *Valve* provide parental controls, age gating, or child profiles that moderate the type of content restricted accounts can access.

Meta Quest 2 The *Meta Quest 2* device does not allow children under the age of 13 to create primary accounts. However, with the Meta Quest 2, a user can add up to three additional accounts to their device. The primary account on the device can add additional accounts in VR. All accounts will need either a Meta account or optional Facebook account to have their own unique account settings and profile. Meta's policies say that additional accounts will be able to install and use apps that they have purchased from the Oculus store, as well as apps purchased by the primary account if app sharing is turned on. Additional accounts can save their own app progress, media files and make use of social platform features like parties, leaderboards and achievements, as well as creating and customizing their own avatar. Apps installed by additional accounts won't take up extra storage space on the device if the admin account already has the app installed.

However, Meta recently launched a new set of parental supervision tools for teens over the age of 13[169] and a parent education hub through the companion software Oculus app.[170] The new suite of parental control tools requires parents to connect to their teen's account and then allow parents to set age-appropriate content settings, restrict third-party purchases and downloads, set time limits on the amount of time spent in VR, see their teen's friends list in the companion Messenger app and who they're interacting with in VR. In addition, parents will be able to view their teen's headset VR experience and screen time from the Oculus mobile app.

PlayStation VR The *PlayStation VR* provides parental controls through a feature called Family Management through which parents can restrict content, such as games and movies, and keep track of and limit playtime. Parents can also use a shared wallet and set spending limits with their children and can restrict communication features, such as chatting and messaging. The PlayStation also provides Family and Parental Controls with PS5 Console Restrictions that restrict user creation and guest logins to the device, and sets default parental controls for new users of the console.

To create a child account or profile on the PlayStation, the parent or guardian is required to first navigate to a website on another device and select Family Management to create a child account or invite an adult with an existing account.[171] A parent can scan a QR or navigate directly to the website on another device and is required to log in with their username and password. The parent is asked to provide the birthdate of their child and provides notice that other players won't be able to see the child's account. The PlayStation parent or guardian verification process provides notice that in order to add children to a family, a $.50 charge is necessary to verify that the primary account is an adult. PlayStation says this is only required once as the family manager, and there will be no charge for adding more family members. Lastly, PlayStation provides notice that the charge will be funded to the primary account user's wallet, and they can use it for purchases. Parents need to be aware that they will need to have a credit card on file with PlayStation to complete the verification process.

PlayStation requires parents to enter a valid email address and a secure password for their child, and the email address will be used to send important information. Also family members will be able to see a child's email address, but other players won't. If a child does not have their own email address, then a parent is required to create a seperate email address for PlayStation to contact

[167] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Parts 312.2, 312.3(d), 312.5, 312.5(a), 312.5(b)(1)–(2)(i)–(iv); *See also* 15 U.S.C. § 6501(9).

[168] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.6.

[169] *See* Meta Quest, Introducing VR Parental Supervision Tools on Quest: https://about.fb.com/news/2022/03/vr-parental-supervision-tools-on-quest.

[170] *See* Meta Quest, Parent Education Hub: https://store.facebook.com/quest/safety-center/parental-supervision.

[171] *See* PlayStation Family Account: https://www.playstation.com/acct/family.

them, which may be difficult for younger children who do not use email but wish to play age-appropriate games.

Upon adding a new user account to the PlayStation using their email address and password, a child must update their account that includes their profile information, online ID and avatar, and privacy settings. A child must enter their first and last name, which PlayStation indicates will only be seen by their parents. In addition, the child's postal code, city, and state information is collected by PlayStation to verify their identity if they contact them.

The child can choose an avatar icon and can choose an online ID. Other players will see the online ID in places like games, messages, and searches, and PlayStation recommends that children do not include their real name or personal information. A child must choose a privacy profile as covered in Table 14 that allows them to customize their privacy settings, such as who can see their information and activity when playing games. Parents will receive an account creation confirmation email and must verify the email address can be accessed before the child profile can be activated.

After activation, the child account profile does not display the marketing communications notifications settings, or the personalized advertising settings, indicating to parents that these options have likely been disabled for a child profile. PlayStation provides notice that for use of PlayStation VR, the VR headset isn't for use by children under age 13 without parental consent. Also, for communication and user-generated content, PlayStation restricts chatting and messaging with other players (including a child's friends) as well as viewing or sharing videos, images, and text on PlayStation network. Lastly, PlayStation provides age filtering of online content which includes restricting access to online features of PS4 or PS5 games, and hiding games and content in PlayStation store based on a child's age.

Valve Index The *Valve Index* has parental controls through its integration with Steam Desktop and is managed with a feature called Family View.[172] Family View can be used to restrict access to content and features in the Steam application while in PIN-protected Family View. Parents can restrict what library content a child can view to "only games I choose" or "all games." In addition, parents can select which online content and features children can view such as the Steam store, community-generated content, friends, chat, and groups, their online profile, screenshots, or achievements. The Family View feature in Steam is also available to other VR headsets not manufactured by Valve that access Steam content such as the HP Reverb G2 and HTC Vive Cosmos Elite if using SteamVR to play games. However, the Microsoft Mixed Reality Portal used by the HP Reverb G2 and HoloLens 2, and HTC Viveport used by the HTC Cosmos Elite do not provide parental controls because they are not intended for children under 13 years of age.

[172] *See* Steam Support, Family View: https://help.steampowered.com/en/faqs/view/6B1A-66BE-E911-3D98.

Child and teen privacy protections

If children under the age of 13, or teens younger than 18, use a VR application or device, the company should disclose how they better protect the privacy of children and teens in their privacy policy. In addition, if a VR application or device has worse privacy practices for adult users or consumers such as selling data to third parties or displaying targeted advertising that could inadvertently apply to children, then the company should disclose additional protections are in place to protect those children or teens. Even if a VR application or device is not intended to be used by children or teens, it should still disclose in its privacy policy how it will handle information inadvertently collected from children or teens with stronger privacy protections until it can be deleted.

None of the VR devices we tested disclosed stronger privacy protections in their policies for children or teen users.

Meta Quest 2 The *Meta Quest 2* terms of service say that users under the age of 13 may not create a Facebook account and therefore are not able to log in or create an account with Facebook in order to use the Meta Quest 2 device. However, teens older than 13 but younger than 18 may use the Meta Quest 2 with parental consent and Meta's parent supervision tools. Meta's parental supervision controls provide parents with some important safety features, but also a false sense of privacy, since no additional privacy protections are guaranteed for children or teens. For example, although Meta's parental controls restrict age-inappropriate content and provide transparency into their teen's VR experience, teens are still subjected to commercial monetization practices such as third-party marketing, targeted advertising, tracking, and profiling.In addition, Meta discloses no specific stronger privacy protections for children under the age of 13, or teens between ages 13 and 18. Therefore, the Meta Quest 2 does not meet our recommendations for privacy with children under the age of 13 or teens under 18.

PlayStation VR The *PlayStation VR* privacy policy has a section titled Children's Information, but only discloses that they obtain parental consent for the collection of personal information from children under the age of 13. The policy does not provide any additional information about how they protect the privacy of children under 13 using a child's account or teens between the ages of 13 and 18 years old. PlayStation's policies do not include prohibitions on selling data to third parties or the use of children's or teens' personal information for targeted advertising, tracking, or profiling. Therefore, because

Table 21: Child and teen privacy protections

Device	Children Under 13 Intended	Children Under 13 Protected	Teens Over 13 Intended	Teens Over 13 Protected
Microsoft HoloLens 2	Yes	No	Yes	No
HP Reverb G2	No	No	No	No
HTC Vive Cosmos Elite	No	No	No	No
PlayStation VR	Yes	No	Yes	No
Meta Quest 2	No	No	Yes	No
Valve Index	Yes	No	Yes	No
Pimax Vision 5K	No	No	No	No

PlayStation does not disclose specific and stronger privacy protections for children under the age of 13 or teens under 18, the PlayStation VR does not meet our recommendations for privacy with children or teens.

Valve Index The *Valve Index* privacy policy has a section titled Children, which states the minimum age to create a Steam user account is 13, and that parental consent is obtained for the collection of information from users older than 13. However, the policy does not provide any additional information about how they protect the privacy of children under 13 or teens between the ages of 13 and 18 years old using a restricted Family View account. Steam's policies do not include prohibitions on selling data to third parties or the restricted use of a Family View user's personal information from targeted advertising, tracking, or profiling. Therefore, because Valve does not disclose specific and stronger privacy protections for children under the age of 13, or teens under 18 the *Valve Index* should not be used with children or teens.

HP & HTC The *HP Reverb G2*'s privacy policy has a Children's Privacy section, but only generally says that HP services are made for the general public and they do not knowingly collect data from children without obtaining parental consent. HP is nontransparent about use of its services by teens between the ages of 13 and 18 years old. The *HTC Vive Cosmos Elite* privacy policy does not disclose any information about children and does not disclose whether HTC obtains parental consent in the event they collect personal information from children under the age of 13. In addition, HTC is also nontransparent about use of its services by teens between the ages of 13 and 18 years old. Therefore, because HP and HTC do not disclose specific and stronger privacy protections for children under the age of 13, teens under 18, the *HP Reverb G2* and *HTC Vive Cosmos Elite* does not meet our recommendations for privacy with children or teens.

Microsoft HoloLens 2 The *Microsoft HoloLens 2* privacy policy has a Collection of Data from Children section. The section says Microsoft obtains parental consent for the collection of personal information from children and that they will not knowingly ask children under 13 to provide more data than is required to provide for the product. However, the policy does not disclose additional protections for children under 13 or teens between the ages of 13 and 18 years old. Therefore, Microsoft's policies do not include prohibitions on the use of personal information for targeted advertising or tracking purposes for children under 13 or teens, which Microsoft engages in for other users. A parent or guardian who is the organizer of a Microsoft family group can manage a child's information and settings on their Family Safety page [173] and view and delete a child's data on their privacy dashboard. [174] Therefore, because Microsoft does not disclose specific and stronger privacy protections for children under the age of 13, or teens under 18, the HoloLens 2 does not meet our recommendations for privacy with children or teens.

Pimax Vision 5K The *Pimax Vision 5K* has a very limited section in its privacy policy titled Minors that indicates its websites and services are only intended for "legal persons" over the age of 18 in the United States. Pimax does not disclose any privacy protections for children under 13 or teens who may use the VR device under the age of 18. Therefore, because Pimax does not disclose specific and stronger privacy protections for children under the age of 13, or teens between the ages of 13 and 18 years old, the Pimax Vision 5K does not meet our recommendations for privacy with children or teens.

Advertisements, marketing, and tracking

Responsible advertising practices limit the use of personal information for any first-party or third-party marketing, targeted advertising, tracking, or profiling purposes.

[173] *See* Microsoft Family Safety: https://www.microsoft.com/en-us/microsoft-365/family-safety.
[174] *See* footnote 146.

Marketing

The marketing evaluation questions indicate whether first-party or third-party marketing communications may be sent to users that include emails, text messages, or other app notifications for a product or service. These marketing communications can come from the first-party VR app developer that has a direct relationship with the user and is typically expected by users to include new premium products or services from the app developer that are related to the app they are using and may find useful. In addition, marketing communications can also come from a third-party application or service that a user does not have a direct relationship with and is not expected because the communications are for products or services unrelated to the first-party relationship the user has with the app developer. These third-party marketing communications typically are unexpected and unwanted by users because the first-party app developer shared their personal information with a third-party company without their knowledge to communicate unrelated or unsolicited products or services from third-party companies.[175] Additionally, depending on whether the user is a child, student, or consumer, various state, federal, or international privacy laws may prohibit the use of personal information for third-party marketing communications without consent.[176,177,178,179,180,181]

Meta Quest 2 The *Meta Quest 2* setup process requests opt-in consent to receive emails from Oculus about future releases and sales. The *PlayStation VR* device provides users with a notice to receive marketing messages. The notice states "Would you like to receive information about new products, special offers, and other promotions about PlayStation and Sony from Sony Interactive Entertainment?" Users can change their marketing communication settings under Users and Accounts → Account → Communication Preferences and opt out of receiving marketing communications via email or via notifications on the console.

HTC Vive Cosmos Elite The *HTC Vive Cosmos Elite* setup process requests that users enter their email address and sign up for the HTC Viveport Infinity subscription service for a monthly or annual plan, but users need to find and click "maybe later" to proceed to the next section without subscribing. In addition, during the setup process a marketing communication option is displayed to users that says, "Yes, I want to receive important product updates, news, and exclusive offers related to VR." This third-party marketing option is opt-out by default, meaning the check box is pre checked and requires unchecking the box before proceeding to the next step.

Microsoft HoloLens 2 The *HoloLens 2* requires the use of a Microsoft account which inherits all the default privacy settings from a user's Microsoft Privacy Dashboard. A user can change those settings by logging into their privacy dashboard under promotional communications → review settings → and communication preferences of their email address. A user can opt out to receive "general info and offers from Microsoft" and opt out from "communications from Microsoft partners."

Valve, HP, and Pimax The *Valve Index*, *HP Reverb G2*, and *Pimax Vision 5K* devices did not request the user consent for any first-party or third-party marketing communications at any time during the setup process. In addition, Pimax did not even collect a user's email address, whereas the other devices required users to create an account.

Targeted advertising

Personalized advertising in VR is the practice of displaying targeted commercial advertisements to users for either first-party or third-party products and services in the VR experience based on their collected personal or behavioral information including how users interact in VR. Personalized advertisements can be linked to a specific individual, device, application, or behavioral profile which requires the collection of specific information about users typically through the use of cookies, beacons, tracking pixels, persistent identifiers, fingerprinting, or other tracking technologies.[182]

Virtual reality advertising is different from traditional advertising because it can use extremely specific characteristics and preferences about the user in order to build behavioral virtual reality profiles that can be used to exploit user's characteristics for commercial purposes. This rich VR behavioral information is also shared with third-party advertisers, who can display even more targeted products to the user on other apps or devices

[175] *See* Perrin, A. (2020, April 14). Half of Americans have decided not to use a product or service because of privacy concerns. *Pew Research Center*. https://www.pewresearch.org/fact-tank/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns; *See also* Auxier, A., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November 15). Americans and privacy: Concerned, confused, and feeling lack of control over their personal information. *Pew Research Center*. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information.

[176] *See* footnote 72.

[177] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(1)(A).

[178] *See* footnote 80.

[179] *See* footnote 81.

[180] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(a).

[181] *See* footnote 83; *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(e)(6).

[182] *See* Electronic Frontier Foundation. (2020). What is fingerprinting? https://ssd.eff.org/en/module/what-fingerprinting.

Table 22: Marketing communications

Device	Developer Marketing Setting	Developer Marketing Policy	Third-Party Marketing Setting	Third-Party Marketing Policy
Microsoft HoloLens 2	Opt-out	Yes	Opt-out	Yes
HP Reverb G2	None	Yes	None	Yes
HTC Vive Cosmos Elite	Opt-out	Yes	Opt-out	Yes
PlayStation VR	Opt-out	Yes	Opt-out	Yes
Meta Quest 2	Opt-in	Yes	Opt-in	Yes
Valve Index	None	Yes	None	Unclear
Pimax Vision 5K	None	Yes	None	Yes

outside VR based on the specific behavioral information they received from the user's activities in VR.[183,184,185]

Beyond technical device information, a user's experience in VR has the potential to expose behavioral information that can be used for targeted advertising as well. Due to the inherent functionality of VR, these devices and their applications can collect far more sensitive information and biometric information than mobile devices and applications can. Behavioral information can include the user's height, posture, gaze, gait, gestures, even the distance between your eyes called interpupillary distance (IPD),[186] facial expressions, and more.[187] Studies have shown that behavioral biometric tracking data can be used to uniquely identify users, such as through hand, head, and eye motion data collected from users while performing tasks in VR[188] or while viewing and interacting with 360-degree videos in VR.[189]

VR devices also have different capabilities for positional tracking in order to render the user's position in the VR environment correctly as they move and interact within the real and virtual space. VR systems use either outside-in tracking, such as through cameras or base stations separate from the VR device, or inside-out tracking, such as through cameras on the VR device itself. Base stations, like those used by the *Valve Index*, are positioned in the physical space and use infrared to communicate with the VR device and controllers[190], while outside-in cameras are connected to an external device that is connected to the VR system, such as the PlayStation Camera used with the PlayStation VR device.[191] Inside-out tracking involves cameras on the VR devices themselves pointing outwards into the user's environment.[192] Both methods for positional tracking can potentially expose the user's real-world environment through images or scans from the sensors, since this information is used by the device to render content and track the user's movements for functionality purposes. However, this data can be yet another piece of sensitive information collected by VR devices and apps for profiling and targeted advertising purposes.

While VR devices themselves have the capability to serve ads within the environment, advertisers are continuing to develop new ad formats, such as virtual items,[193,194] virtual rooms,[195] billboards,[196] and even

[183] *See* footnote 72.

[184] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(e)(6), (ah).

[185] *See* footnote 79.

[186] Avi Bar-Zeev. (May 28, 2019). The Eyes Are the Prize: Eye-Tracking Technology Is Advertising's Holy Grail. *Vice.* https://www.vice.com/en/article/bj9ygv/the-eyes-are-the-prize-eye-tracking-technology-is-advertisings-holy-grail.

[187] *See* footnote 50.

[188] Pfeuffer, K., Matthias, J., Geiger, M.J., Prange, S., Mecke, L., Buschek, D., & Alt, F. 2019. Behavioural biometrics in VR: Identifying people from body motion and relations in virtual reality. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19).* Association for Computing Machinery. https://doi.org/10.1145/3290605.3300340.

[189] Miller, M.R., Herrera, F., Jun, H., Landay, J.A., & Bailenson, J. (2020, October 15). Personal identifiability of user tracking data during observation of 360-degree VR video. Sci Rep 10, 17404. https://doi.org/10.1038/s41598-020-74486-y.

[190] *See* Valve Index Base Stations: https://www.valvesoftware.com/en/index/base-stations.

[191] *See* PS VR: PlayStation Camera Setup: https://www.playstation.com/en-us/support/hardware/ps4-playstation-camera-setup-for-ps-vr/.

[192] *See* Inside-out tracking, https://docs.microsoft.com/en-us/windows/mixed-reality/enthusiast-guide/tracking-system.

[193] Forbes. (2021). *10 ways virtual reality will impact the future of advertising.* https://www.forbes.com/sites/forbesagencycouncil/2021/05/13/10-ways-virtual-reality-will-impact-the-future-of-advertising/.

[194] Dang, S. (2022, March 24). Meta inks partnership for 3D ads in step toward the metaverse. *Reuters.* https://www.reuters.com/technology/3d-ads-come-facebook-instagram-step-toward-metaverse-2022-03-24/.

[195] "The Virtual Room ad: a real way to make money in VR." Unity. https://create.unity.com/virtual-room-ad.

[196] Stein, S. (2021, June 23). Facebook's VR advertising plans feel inevitable, but it's starting off rocky. *CNET.* https://www.cnet.com/tech/computing/facebooks-vr-advertising-plans-feel-inevitable-but-its-starting-off-rocky.

stores [197] and restaurants, [198] that allow users to interact with ads within third-party VR apps and spaces, enabling companies and developers to generate revenue just like in mobile applications. [199]

Currently, advertising in VR can often seem out of place in the environment and destroy the immersive experience when visual or auditory advertising is forced into their field of view or experience. However, if sensitive and biometric information collected in VR is able to be captured through user interactions and behaviors with virtual ads, this data can also be used to create extremely detailed profiles of users for profiling and targeted advertising purposes. Additionally, such novel VR ad formats may be difficult for users–particularly children–to identify as ads, which may cause users to interact more with ads or content they believe as part of the game or experience and provide even more sensitive information for advertising purposes. [200]

Some traditional video games have also come under fire for displaying ads that confuse regular game play with ads since they are not clearly marked, [201] which may happen in VR as well and be even more confusing in VR games that use such new and interactive ad formats. Over time, users may become more desensitized to the placement and interaction with advertising in VR environments and overall lower their expectations of privacy in this new virtual reality environment.

VR ads in apps and games could also exploit such rich behavioral user data to persuade or encourage specific actions, interactions, or in-app purchases, such as through digital items, loot boxes, virtual avatar clothing or customizations, and more. Indirect or inadvertent interactions with VR ads or content can be used for highly detailed profiling that in both virtual reality and the real world is used to define a user's identity; such as their gaze, how long they look at a product, what part of the product they look at, the objects with which they interact, and how they interact with objects.

Interacting with ads and ad products in VR games could be used to provide bonus points or extra features unavailable to other players, thereby increasing the likelihood of users interacting with ads and marketing, or providing opt-in consent to experience an ad at the very moment when they are most susceptible (e.g. when they have low battery, or low health and are about to fight the final boss). These types of in-app incentives could disproportionately target vulnerable users with more advertising and marketing interactions, which could serve to increase contextual harms, both of inclusion and exclusion, and give rise to amplifying patterns of discrimination and disadvantage. [202]

Beyond VR ads, metadata and analytics about a user's VR app usage, friends list, and interactions with other users, such as which apps are opened, when, where, and for how long messaging metadata, messaging content, or even transcribed voice communication, could be used for advertising profiles. Additionally, VR devices like the Meta Quest 2, PlayStation VR, and HoloLens provide their own integrated web browser interface which could enable advanced tracking that includes which web pages and content users choose to access in VR for advertising and profiling purposes. Additional third-party apps that provide web browsing, screen sharing, or collaboration tools could also use the activity and content viewed by users for advertising purposes. Moreover, a user's behavioral data tracked in the VR environment could be used to exploit their decision-making ability outside of VR, such as while browsing the web on another computer or mobile device, to serve targeted ads and marketing for products and services, likely persuading users through gamification to save money on certain apps in VR for a limited time, or to purchase new virtual items to compete with their friends and level-up to keep kids coming back to VR. This new type of *virtual reality biometric-derived advertising* will redefine a new category of data and behavioral monetization, and manipulation.

The most popular VR devices we tested displayed first-party advertising and third-party advertising in different ways and for different purposes. For example, standalone devices, like the Meta Quest 2, displayed advertising in the VR experience, but tethered VR devices displayed advertising in their companion software or respective App Stores on the user's personal computer. Several VR devices did not provide any privacy controls to limit a user's data for advertising purposes either through the device or app store. Both the HTC Vive Cosmos and Microsoft HoloLens provided opt-out privacy settings, which means a user's sensitive data can still be used for advertising purposes until the user restricts the use of their data. Only PlayStation provided better privacy protecting opt-in settings for their sensitive data to be used for advertising purposes, which is a privacy-by-design principle because it does not inadver-

[197] McDowell, M. (2021, November 24). Virtual stores: Fashion's new mode of shopping. *Vogue Business*. https://www.voguebusiness.com/technology/virtual-stores-fashions-new-mode-of-shopping. *See also* Murphy, H. (2022, January 17). Facebook patents reveal how it intends to cash in on metaverse. *Financial Times*. https://www.ft.com/content/76d40aac-034e-4e0b-95eb-c5d34146f647.

[198] Alcántara, A.M. (2022, April 5). Restaurants' virtual stores test consumers' appetite for metaverse marketing. *Wall Street Journal*. https://www.wsj.com/articles/restaurants-virtual-stores-test-consumers-appetite-for-metaverse-marketing-11649160001.

[199] Parlock, J. (2021, June 17). Facebook is experimenting with placing ads within VR apps. *Forbes*. https://www.forbes.com/sites/joeparlock/2021/06/17/facebook-is-experimenting-with-placing-ads-within-vr-apps/.

[200] *See* footnote 48.

[201] Deighton, K. (2022, April 22). Companies try to sell videogaming as the next big advertising channel. *Wall Street Journal*. https://www.wsj.com/articles/companies-try-to-sell-videogaming-as-the-next-big-advertising-channel-11650621600.

[202] *See* Milano, S., Mittelstadt, B., Wachter, S., & Russell, C. (2021, June 17). Epistemic fragmentation poses a threat to the governance of online targeting. *Nat Mach Intell* 3, 466–472. https://doi.org/10.1038/s42256-021-00358-3.

tently use users' data for advertising purposes prior to receiving their explicit consent.

Meta Quest 2 The *Meta Quest 2* device displays first-party advertising to remind a user to install the social networking app Facebook [203] and should register an account before they set up and use the VR device. This is an example of a potential "dark pattern" that by design is not privacy-protective because it encourages users to sign up for a separate Facebook account with different privacy settings and Facebook is not clear about how a user's Facebook privacy settings will impact the Quest 2 device. However, Meta has recently added a new feature to create Meta accounts with the Quest 2 without the need for a Facebook account. [204] The Quest 2 device displays first-party advertising to persuade the user to install another first-party app called Messenger [205] to enable social interactions and chat features in Facebook and in the Quest 2 VR experience and within third-party VR games. Lastly, the Meta app store displays and promotes sponsored third-party advertisements for VR applications to purchase. There are no privacy settings in the VR experience to either opt in or opt out of the use of a user's data for advertising purposes. However, users can change their Facebook privacy controls for advertising and marketing purposes which are inherited by their Oculus account, but it is not clear in Meta's privacy policy how changing Facebook related advertising settings may or may not impact use of the Quest 2 device. In addition, at the time of testing it was not possible to determine if new advertising and marketing controls will be available for the new Meta accounts The lack of opt-in or opt-out advertising settings in the VR experience is not a privacy-by-design best practice and does not provide any control for the user to control how their sensitive data is used by Meta for advertising purposes.

PlayStation VR The *PlayStation VR* device displayed first-party advertisements within the PlayStation Home screen for the PlayStation Plus subscription service [206] that provides access to hundreds of PlayStation games to play for one monthly price with online multiplayer features that include social interactions provided through the PlayStation Network. [207] In addition, the PlayStation store available on the console device displays third-party advertisements for sponsored games to purchase. The PlayStation "*Personalized Advertising*" privacy setting by default is disabled and provides notice that if enabled PlayStation may "show you personalized ads (sometimes assisted by data from third-party sources) in our products and services, and on third-party apps and sites. When this setting is disabled, you'll still see ads, but they may be less relevant." This default setting is an example of privacy by design, but if enabled would allow PlayStation to customize advertising on other apps and services across the internet based on tracking your behavioral data while using the gaming console or VR device.

Valve Index The *Valve Index* displays first-party advertisements to purchase the *Valve Index* VR device in the Steam App Store and additional Steam related products such as the Steam Deck. In addition, the SteamVR app store displays and promotes sponsored third-party advertisements for VR applications to purchase. There are no privacy settings in the desktop Steam App Store to either opt in or opt out of the use of a user's data for advertising purposes. This is not a privacy-by-design best practice and does provide any control to the user over how their sensitive data is used.

HP Reverb G2 The *HP Reverb G2* Mixed Reality Portal displays third-party advertisements for games from the SteamVR app store, but does not display any first-party HP related advertisements to purchase additional products or services from HP. The Reverb G2 also utilizes the Microsoft Mixed Reality desktop launcher with the App Store which displays third-party advertisements for VR applications. There are no privacy settings in the VR experience to either opt in or opt out of the use of a user's data for advertising purposes. This is not a privacy-by-design best practice and does provide any control to the user over how their sensitive data is used.

HTC Vive Cosmos Elite The *HTC Vive Cosmos Elite* displays first-party advertising during the setup process to subscribe to its HTC Infinity subscription service. In addition, third-party advertisements are displayed in the HTC Viveport store to purchase additional VR apps and content from various third-party developers. The *HTC Vive Cosmos* has privacy controls in the companion Viveport software, which has a "Personalized Experience" setting in the "My Profile" section. The "Personalized Customer Experience" is pre-checked, meaning the default setting is opt-out, which is not a privacy-by-design best practice. The personalization setting says "utilize and apply information related to my use of HTC devices and services to improve my personalized experience across all HTC services such as sending information and offers that are relevant to me."

Microsoft HoloLens 2 The *Microsoft HoloLens 2* did not display any firsty-party advertising during the HoloLens setup process. However, the device requires the use of a Microsoft account which inherits all the default advertising privacy settings from a user's Microsoft account Privacy Dashboard. A user can change those settings by logging into their privacy dashboard under privacy,

[203] *See* Facebook: https://www.facebook.com.
[204] *See* footnote 159.
[205] *See* Messenger: https://apps.apple.com/us/app/messenger/id454638411; Google Play Store, Messenger: https://play.google.com/store/apps/details?id=com.facebook.orca&gl=US.
[206] *See* PlayStation Plus: https://www.playstation.com/en-us/ps-plus.
[207] *See* PlayStation Network: https://www.playstation.com/en-us/playstation-network.

Table 23: First- and third-party advertising displayed

Device	First-Party Ads	Third-Party Ads	Ad Settings
Microsoft HoloLens 2	No	Yes	Opt-out
HP Reverb G2	No	Yes	None
HTC Vive Cosmos	Yes	Yes	Opt-out
PlayStation VR	Yes	Yes	Opt-in
Meta Quest 2	Yes	Yes	None
Valve Index	Yes	Yes	None
Pimax Vision 5K	No	Yes	None

then ad settings. Microsoft provides users with the opt-out choice to "see ads that interest you." Microsoft says they can use your searches, past purchases of Microsoft products, and other online activity associated with both your Microsoft account and this browser to show you ads that are more personalized. If you've allowed Microsoft Edge to use your browsing activity for personalized web experiences, Microsoft can also use your Microsoft Edge browsing activity to personalize ads. Even if you turn off this setting, you may still see personal ads from other companies based on information they have collected from you.[208]

The Microsoft HoloLens 2 device uses Microsoft Edge as its primary web browser and therefore would allow Microsoft to use all web browsing activity performed while using a HoloLens to be used for targeted advertising. In addition, the HoloLens has a "Settings" application which provides more advertising related settings. Under Privacy, then change privacy options, Microsoft provides users with an opt-out choice to "let apps use the advertising ID of the HoloLens device to make ads more interesting to you based on your app activity." In addition, Microsoft provides a second opt-out choice to let Windows track app launches to improve Start and Search results. During the HoloLens setup-process Microsoft provides an opt-in choice to let Microsoft and apps use your location information to receive location-based experiences or use other services that require your location to work.

Lastly, during the setup process Microsoft provides an opt-out choice to collect "Optional diagnostic data" (default selection) which sends all "required diagnostic data," along with additional information about websites you browse and how you use apps and features on the device, plus additional information about device health, device activity and enhanced error reporting. The alternative choice is to only select "required diagnostic data" that sends only information about your device, its settings and capabilities, and whether it is performing poorly. In addition, there is a separate diagnostic related privacy setting under the Settings application under the Diagnostic & Feedback section. Microsoft provides users with the opt-out choice to receive "tailored experiences that let Microsoft use your diagnostic data, excluding information about websites you browse, to offer you personalized ads and recommendations to enhance your Microsoft experience."

Pimax Vision 5K The *Pimax Vision 5K* device setup process using Pitool did not display any first-party or third-party advertisements and the device is primarily a value-added retailer designed to work with SteamVR or Oculus desktop app to access a user's content library. There are no privacy settings in the desktop SteamVR App Store or Oculus desktop app to either opt in or opt out of the use of a user's data for advertising purposes. This is not a privacy-by-design best practice and does not provide any control to the user over how their sensitive data is used.

Tracking and profiling

The practice of tracking is when the VR device or application allows companies to use cookies or other tracking technologies on its product, which enables those companies to collect and use a user's personal information for their own commercial purposes. Data collected from tracking can be used to influence a user's decision-making processes without their knowledge, which may cause unintended risks, and may be particularly concerning when this happens via third parties.[209,210] Profiling users is when a VR device or application allows third-party companies to create a behavioral or sensitive biometric profile about a user based on the user's personal information or activity in VR for advertising or marketing purposes over time across the internet.

Our observational analysis and classification of advertising and tracking domains that were communicated with by each virtual reality device and application is displayed in Table 24. We indicate whether any primary domains are classified as trackers, based on the open source Tracker Radar project from DuckDuckGo.[211] The Tracker Radar tool is not a block list, but a data set of the

[208] *See* footnote 146.

[209] *See* footnote 88.

[210] *See* footnote 89.

[211] *See* DuckDuckGo Tracker Radar: https://github.com/duckduckgo/tracker-radar.

Table 24: Tracking on VR devices. Tracking behavior based on domain or primary domain contacted Abbreviated columns are as follows: (AP) Action Pixels, (AF) Ad Fraud, (AMT) Ad Motivated Tracking, (AD) Advertising, (AM) Audience Management, (SN) Social Network, (TPAM) Third-Party Analytics Marketing. For further explanation, see appendix Tracking Categories.

Device	AP	AF	AMT	AD	AM	SN	TPAM
Microsoft HoloLens	Yes	Yes	Yes	Yes	No	No	No
HP Reverb G2	Yes	Yes	Yes	Yes	No	No	No
HTC Vive Cosmos Elite	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PlayStation VR	No	No	Yes	Yes	Yes	No	Yes
Meta Quest 2	Yes	Yes	Yes	Yes	Yes	Yes	No
Valve Index	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Pimax Vision 5K	No	No	Yes	Yes	Yes	No	No

tracker and tracker-like behavior that is continually updated and analyzed to reflect new tracking behavior.[212]

Each observed domain in our security testing is classified by Tracker Radar into the following advertising and tracking categories that are relevant to virtual reality devices: **AP**: Action Pixels; **AF**: Ad Fraud; **AMT**: Ad Motivated Tracking; **AD**: Advertising; **AM**: Audience; Measurement; **SN**: Social Networking; and **TPAM**: Third-Party Analytics Marketing.[213] Additional information about the classification of each domain for each virtual reality companion application or virtual reality device is available in the Appendix.

Observing first- or third-party trackers is an important step in validating a product's privacy practices, but it is also an ephemeral process that is constantly changing. Tracking the trackers is a narrow snapshot of behavior in time analyzed relative to the most up-to-date knowledge we have of each particular domain's past behavior.

It is also important to understand that the presence of trackers in each classification only looks at unique primary domains and not their subdomains, which could have multiple requests and be used for a potentially nontracking purpose. In addition, a domain may not be counted as a tracker in our analysis because Tracker Radar has not yet collected information about that particular domain or subdomain with DuckDuckGo's Tracker Radar Collector.[214] Moreover, Tracker Radar is a data set of the most common third-party domains on the web, which was not necessarily designed to apply to known tracking domains from virtual reality applications and devices. However, our analysis still indicates that virtual reality apps and devices that use trackers should be more carefully scrutinized by parents and educators before use, and their privacy policies carefully read to better understand their privacy practices. Lastly, our observational results of trackers are simply a snapshot of behavior we observed from a virtual reality app or device on a specific date and time in our particular network environment; the traffic observed would likely change based on different testing configurations or real world use.

This observational data, as summarized in Table 24 can be used to roughly validate whether each VR device's third-party tracking practices are consistent with their privacy policy and whether they disclose that they engage in third-party tracking for advertising purposes. All of the VR devices we tested were observed transmitting requests to known tracking-related domains. In some cases as few as three tracking domain categories were observed, and in other cases all seven tracking categories were observed.

All VR devices we tested were observed sending requests to domains classified as tracking domains for commercial purposes.

Most of the VR device's respective privacy policy also disclosed that they can use data from a user's VR experiences for third-party tracking purposes which aligns with our observations. It should be noted that the *Pimax* includes tracking-related requests from its Pitool companion software used to integrate with SteamVR. In addition, only the *Valve* and *Pimax* devices were nontransparent in their privacy policies on the issue of third-party tracking, but our observational analysis shows that both these devices' use of SteamVR resulted in communication with third-party domains known to engage in tracking for commercial purposes. This provides further

[212] *See* DuckDuckGo. (2022, August 5). More privacy and transparency for DuckDuckGo web tracking protections. https://spreadprivacy.com/more-privacy-and-transparency/.
[213] *See* DuckDuckGo Tracker Radar, Categories: https://github.com/duckduckgo/tracker-radar/blob/main/docs/CATEGORIES.md.
[214] *See* DuckDuckGo Tracker Radar Collector: https://github.com/duckduckgo/tracker-radar-collector.

Table 25: Tracking on VR companion apps. Tracking behavior based on domain or primary domain contacted Abbreviated columns are as follows: (AP) Action Pixels, (AF) Ad Fraud, (AMT) Ad Motivated Tracking, (AD) Advertising, (AM) Audience Management, (SN) Social Network, (TPAM) Third-Party Analytics Marketing. For further explanation, see appendix Tracking Categories.

Product	AP	AF	AMT	AD	AM	SN	TPAM
Oculus desktop app	Yes	Yes	Yes	Yes	Yes	Yes	No
Oculus app	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Facebook app	Yes	Yes	Yes	Yes	Yes	Yes	No
Messenger app	Yes	Yes	Yes	Yes	Yes	Yes	No
PlayStation app	Yes	No	Yes	Yes	Yes	No	Yes
SteamVR desktop app	No	No	Yes	Yes	No	No	No
Windows Mixed Reality desktop app	Yes	Yes	Yes	Yes	No	No	No
HTC Viveport desktop app	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft App Store	Yes	Yes	Yes	Yes	Yes	No	No
Pimax Pitool desktop app	No	No	Yes	Yes	Yes	No	No

evidence for the conclusion that when a company's privacy policy does not disclose an important issue such as third-party tracking, they still reserve the right to engage in the practice which can sometimes be verified with observational analysis. [215]

The observational data summarized in Table 25 can be used to validate, in some cases, that each VR companion app's third-party tracking practices are consistent with their privacy policy and whether they disclose that they engage in third-party tracking for advertising purposes. Similarly, to the VR devices, all of the VR companion apps we tested were observed transmitting requests to known tracking domains. In some cases as few as two tracking domain categories were observed and in other cases all seven tracking categories were observed. In addition, most of the VR companion apps' privacy policy also disclosed that they can use data from a user's VR experiences for third-party tracking purposes.

Users are tracked from the moment they put on their VR devices and when they use VR companion software to support their devices and access content.

In addition, in order to download and install many of these VR companion desktop and mobile applications a user is required to navigate to the VR device manufacturer's online website or App Store in order to download and use with their VR device. This action can independently expose users to additional third-party tracking domains on the respective websites or app stores; this additional tracking is outside the scope of this observational analysis.

[215] *See* footnote 103.

Software updates

Evaluating software updates takes into consideration best practices of keeping a virtual reality device secure with encrypted up-to-date software patches and settings. When a company improves its app or device, better privacy and security should be part of the improvements and updates should be automatically applied or easy to apply manually.

Table 26: Software or Firmware Updates for VR device are secure. 'No' indicates that none of the observed updates were served over secure connections. 'Yes' indicates that all of the observed updates were served over secure connections. 'Mixed' indicates that both secure and insecure updates were observed.

Device	Encrypted Updates
Microsoft HoloLens 2	No
HP Reverb G2	Yes
HTC Vive Cosmos Elite	Mixed
PlayStation VR	No
Meta Quest 2	Yes
Valve Index	Yes
Pimax Vision 5K	Yes

The data flows of each VR device were monitored before, during, and after each firmware or software update to determine whether the update was transmitted over encrypted connections. We observed that the *PlayStation VR*, *HTC Vive Cosmos*, and *Microsoft HoloLens 2* did not properly encrypt some or all software or firmware updates incoming to the VR devices. It is possible that VR device manufacturers use alternative security practices

such as software or firmware file signatures, or checksums to verify the integrity of the content of updates. However, this is not considered a security best practice because firmware updates to the VR devices or wireless controllers could be intercepted and compromised while in transit.

The *PlayStation VR* firmware updates and wireless controller software updates were observed transmitted over the internet without encryption. The *HTC Vive Cosmos* was observed downloading base station firmware updates and controller firmware updates with encryption. However, the optional HTC Vive wireless adapter software was downloaded over an unencrypted connection. The *Microsoft HoloLens 2* software updates through Windows Update were observed transmitted over the internet without encryption.

The following companion mobile and desktop applications support all the VR devices and allow access to various App Stores and content libraries:

Table 27: Software and Updates for Apps are secure. 'No' indicates that none of the observed updates were served over secure connections. 'Yes' indicates that all of the observed updates were served over secure connections. 'Mixed" indicates that both secure and insecure updates were observed.

Product	Encrypted Updates
Microsoft App Store	No
Microsoft Mixed Reality	Yes
HTC Viveport	Mixed
PlayStation App	Yes
Facebook	Yes
Messenger	Yes
Oculus Home	Yes
SteamVR Desktop	Yes
Pitool	Yes

Third-party applications

The privacy and security practices of the virtual reality devices we tested only apply to the devices themselves and not to any additional third-party applications or content that may be installed or accessed by the headset from an App Store. Use of any additional third-party VR applications from the Meta, Steam, or Microsoft App Stores include the respective application's own privacy policies and different data collection and use practices. New third-party apps may also have their own privacy settings that need to be configured to minimize data collection and use of a user's data in VR for various concerns including targeted advertising. In addition, some VR devices have first-party social collaborative apps such as Meta's Horizon Worlds[216,217] and Microsoft's AltspaceVR[218] which have the same privacy practices as their parent company. The following basic privacy evaluations[219] of a sample of five of the most popular third-party VR applications[220] with children and students helps illustrate the additional privacy challenges and risks that parents and educators face as they decide which additional apps to install or access in various App Store categories. We evaluated YouTube VR[221] that displays 3D videos in VR, Tilt Brush[222] that allows users to create interactive content in VR, Beat Saber[223] which is a VR rhythm game where users slash the beats of music as they fly toward you, Engage[224] which is a real-time virtual communication platform for business meetings and educational training, and finally VR Chat[225] which is used for social interactions with avatars in VR.

With any third-party VR application a user purchases or downloads they must first provide consent to the additional policies which may have different privacy collection and data use practices then the VR device. Users are therefore expected to read and understand all the policies that apply to their VR device before use, and read the additional policies that apply to each third-party VR application they use. Prior research indicates that the majority of products have a privacy policy reading time of at least 30 minutes.[226]

YouTube VR requires users to provide consent to Google's Privacy Policy,[227] YouTube's Terms of Service,[228] and Community Guidelines.[229] Tilt Brush by Google requires users to provide consent to Google's Privacy Policy[230] and Terms of Use.[231] Beat Saber

[216] *See* footnote 159.
[217] *See* Hill, Kashmir. (2022, October 7). This Is Life in the Metaverse. *New York Times*. https://www.nytimes.com/2022/10/07/technology/metaverse-facebook-horizon-worlds.html
[218] *See* AltspaceVR: https://altvr.com.
[219] *See* Common Sense Privacy Program, Basic and Full Evaluations: https://privacy.commonsense.org/resource/evaluation-framework.
[220] This sample of popular third-party VR applications with children and students was taken from surveys from Educators on VR use in the classroom and the Oculus App Store, PlayStation VR Store, and SteamVR store as of Q2 2022.
[221] YouTubeVR by Google: https://vr.youtube.com.
[222] *See* Tiltbrush by Google: https://www.tiltbrush.com.
[223] *See* Beat Saber: https://www.beatsaber.com.
[224] Engage, https://engagevr.io; *See* Engage, https://www.viveport.com/apps/7c4bdeb9-5f62-470d-a763-34e2b2a170cf.
[225] *See* VRChat: https://hello.vrchat.com.
[226] *See* the "Reading Statistics" section of the 2021 State of Kids' Privacy report: https://www.commonsensemedia.org/research/state-of-kids-privacy-report-2021.
[227] *See* Google Privacy Policy: https://policies.google.com/privacy?hl=en.
[228] *See* YouTube, Terms of Service: https://www.youtube.com/t/terms.
[229] *See* YouTube, Community Guidelines: https://www.youtube.com/howyoutubeworks/policies/community-guidelines.
[230] *See* footnote 227.
[231] *See* Google Terms of Use: https://policies.google.com/terms?hl=en.

Table 28: Privacy rating criteria of virtual reality third-party apps

Product	Privacy Rating	Sell Data	Third-Party Marketing	Targeted Ads	Third-Party Tracking	Track Users	Ad Profile
YouTube Vr[a]	71% Warning	No	Yes	Yes	Yes	Yes	Yes
Tilt Brush[b]	71% Warning	No	Yes	Yes	Yes	Yes	Yes
Beat Saber[c]	30% Warning	Unclear	Unclear	Unclear	Unclear	Unclear	Unclear
Engage[d]	43% Warning	Unclear	Yes	Yes	Yes	Yes	Unclear
VR Chat[e]	46% Warning	No	Yes	Yes	Yes	Unclear	Unclear

[a] *See* Common Sense Privacy Evaluation for YouTube VR https://privacy.commonsense.org/evaluation/YouTube-VR.
[b] *See* Common Sense Privacy Evaluation for Tilt Brush https://privacy.commonsense.org/evaluation/Tilt-Brush.
[c] *See* Common Sense Privacy Evaluation for Beat Saber, https://privacy.commonsense.org/evaluation/Beat-Saber.
[d] *See* Common Sense Privacy Evaluation for Engage, https://privacy.commonsense.org/evaluation/Engage.
[e] *See* Common Sense Privacy Evaluation for VRChat, https://privacy.commonsense.org/evaluation/VR-Chat.

requires users to provide consent to its Privacy Policy,[232] EULA,[233] and Supplemental Beat Saber California Privacy Notice.[234] Engage requires users to provide consent to its Privacy Policy[235] and Terms and Conditions.[236] VR Chat requires users to provide consent to its Privacy Policy,[237] Terms of Service,[238] and Video Content Guidelines.[239]

Youtube VR, Tilt Brush by Google, and VR chat are popular third-party VR applications intended for kids and teens that disclose they do not sell users' data, which is promising. However, both YouTubeVR and Tilt Brush disclose that all data collected by their applications can be used for third-party marketing, targeted advertising, tracking, and profiling for commercial purposes. VR Chat has similar worse privacy protecting disclosures that collected data can be used for third-party marketing and targeted ads but is unclear on the issues of tracking and profiling. Engage is another popular third-party VR application with students for educational training, but their policy is unclear whether student data can be sold to third parties. However, Engage does disclose that users' data can be monetized for third-party marketing, targeted advertising, and tracking purposes. Lastly, Beat Saber is a popular VR game intended for kids and teens and available across multiple VR devices and VR App Store platforms. Beat Saber received the lowest overall score in this comparison of popular VR applications because they were unclear on all of our rating criteria meaning there can be no expectation or accountability of how a user's data will be used by the app for commercial purposes.

Popular third-party VR applications may send and receive their own requests to arbitrary third-party domains which may include known tracking domains with Tracker Radar. Even if a virtual reality device and companion software have better privacy protecting practices for kids and families, the App Store that the virtual reality device connects to for applications and content can still allow third-party applications to be installed or accessed by the device with potentially worse privacy practices than the VR device. Manufacturers of VR devices need to provide clear information about the privacy practices of third-party VR applications in their respective App Stores with easy to read privacy labels and summaries so users can make informed decisions.

The Apple Mac and iOS App Store recently launched its own App Privacy section or "privacy nutrition label" to help consumers understand each app's data collection practices.[240] Google also launched its own Data Safety section in the Google Play Store to help consumers understand each app's privacy and data collection practices.[241] Manufacturers of VR devices could adopt similar App Store privacy nutrition labels or data safety sections for all VR applications to help build consumers' trust and confidence with VR and also support developer's compliance obligations by validating that the VR app's privacy practices are consistent with the their privacy label.[242] Without improvements to the current

[232] *See* Beat Saber Privacy Policy: https://store.facebook.com/legal/quest/beat-saber-privacy-policy.
[233] *See* Beat Saber End User License Agreement: https://store.facebook.com/legal/quest/beat-saber-end-user-license-agreement.
[234] *See* Supplemental Beat Saber California Privacy Notice: https://store.facebook.com/legal/quest/beat-saber-ccpa.
[235] *See* Engage Privacy Policy: https://engagevr.io/privacy-policy.
[236] *See* Engage Terms and Conditions: https://engagevr.io/terms-conditions.
[237] *See* VR Chat, Privacy Policy: https://hello.vrchat.com/privacy.
[238] *See* VR Chat, Terms of Service: https://hello.vrchat.com/legal.
[239] *See* VR Chat, Video Content Guidelines: https://hello.vrchat.com/video-content-guidelines.

[240] Apple. (2022, February 9). *About privacy information on the App Store and the choices you have to control your data.* https://support.apple.com/en-us/HT211970.
[241] *See* Google Play Help, "Understand App Privacy & Security Practices with Google Play's Data Safety" section: https://support.google.com/googleplay/answer/11416267. *See also* Google Play Console Help, "Provide Information for Google Play's Data Safety" section: https://support.google.com/googleplay/android-developer/answer/10787469.
[242] *See* Li, Y., Chen, D., Li, Tianshi, Agarwal, Y., Cranor, L., & Hong, J.I. (2022, April 28). Understanding iOS privacy nutrition labels: An

Table 29: Tracking on VR third-party apps. Tracking behavior based on domain or primary domain contacted Abbreviated columns are as follows: (AP) Action Pixels, (AF) Ad Fraud, (AMT) Ad Motivated Tracking, (AD) Advertising, (AM) Audience Management, (SN) Social Network, (TPAM) Third-Party Analytics Marketing. For further explanation, see appendix Tracking Categories.

Third-Party App	VR Device	AP	AF	AMT	AD	AM	SN	TPAM
YouTube VR	Valve Index	No	No	Yes	Yes	No	No	No
Tilt Brush	Meta Quest 2	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Beat Saber	PlayStation VR	No	No	No	No	No	No	No
Engage	HTC Vive Cosmos	Yes	Yes	Yes	Yes	No	No	No
VR Chat	Pimax Vision 5K	Yes	Yes	Yes	Yes	Yes	No	Yes

status quo; the amount of time required to read third-party VR app privacy policies and the lack of accessible information about privacy will continue to be a barrier for consumers to understand VR device and app privacy practices. Ultimately, this could lead to the widespread adoption of VR devices and applications with worse privacy protections that are inconsistent with consumers expectations and preferences.

In addition, the *Meta Quest 2* App Store provides a third-party "App Lab" section which is a different way for app developers to distribute their beta or demo VR apps directly to consumers for feedback with direct links or platforms like SideQuest,[243] without requiring Meta App Store approval and without sideloading.[244] These third-party apps are available to any user who accepts the risk of installing an app from an unknown developer, but requires caution because these apps present additional security and privacy risks. Any future VR app privacy label requirements that apply to approved apps in the Meta App Store should also apply to any third-party beta or demo apps in the "App Lab" section so users can make a better informed decision to use a product and apps can be removed from the App Lab by Meta for false or misleading privacy practices. Otherwise the third-party App Lab section could quickly turn into the "Malware App Lab" section.

However, some companies are empowering users to push back on their mobile devices. Apple's recent launch of its App Tracking Transparency (ATT)[245] feature requires third-party applications to request that iOS users opt-in to allow a product to track them for advertising purposes using the Identifier for Advertisers (IDFA), which is a unique device identifier Apple generates and assigns to every device. However, there are still other forms of third-party tracking technologies available to companies beyond the IDFA, and many are in use in products that are intended for children and students. Manufacturers of VR devices could adopt similar operating system level privacy-protecting "no tracking" options to prevent third-parties applications from using a user's VR data for any advertising or marketing purposes. This is a continually evolving problem space with new VR devices, new types of identifiers, and new technologies like fingerprinting that will continue to change and need to be considered in future privacy-preserving features.

Third-party applications can include their own requests to third-party tracking domains or include third-party SDKs in their code that make their own tracking requests for advertising or marketing purposes. Popular third-party VR applications were observed during testing using different VR devices to determine whether each application sent tracking-related requests to known categories of third-party domains with Tracker Radar. This type of observational testing requires additional segmentation and analysis because it combines both the requests from the VR device headset, companion VR software, and third-party application into a single black box[246] data flow to determine whether *any* tracking related requests were detected. This method could inadvertently indicate tracking-related requests are present although they originated only from the VR headset, only from the third-party app, or for both. For more information, please see the Appendix for each third-party application to examine which specific domain was associated with tracking-related categories of known tracking domains.

Users should be aware that the VR device, companion VR software, and third-party applications they use all track their activity for commercial purposes.

Similarly to our tracking-related findings for VR devices, all of the third-party applications we tested were

exploratory large-scale analysis of app store data. *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI '22 Extended Abstracts)*. https://doi.org/10.1145/3491101.3519739.

[243] *See* SideQuest: https://sidequestvr.com.

[244] Sideloading typically refers to a media file transfer of an app or other content to a mobile or VR device via USB, Bluetooth, or Wi-Fi that is not vendor-approved.

[245] Apple. (April 2021). *A day in the life of your data – A father-daughter day at the playground*. https://www.apple.com/privacy/docs/A_Day_in_the_Life_of_Your_Data.pdf.

[246] *See* Poston, H. (2020, August 11). What are black box, grey box, and white box penetration testing? Infosec. https://resources.infosecinstitute.com/topic/what-are-black-box-grey-box-and-white-box-penetration-testing.

observed transmitting requests to known tracking domains. In addition, all of the third-party VR apps' privacy policies–except for Beat Saber, which was unclear–disclosed worse practices that they use data from a user's VR experiences for third-party tracking purposes which aligns with our observations. It is important to note that each of the third-party VR app's domain requests were specific to the VR device used and could change if used with a different device. For example, YouTube VR included SteamVR-related domain requests but would likely have included Meta related domain requests if downloaded and used on the Meta Quest 2 instead of from the SteamVR app store.

However, third-party VR apps like Beat Saber used with PlayStation VR were observed sending the majority of their traffic requests to PlayStation-related domains or subdomains, which likely indicates PlayStation was hosting the third-party app through their Content Delivery Network (CDN). Please see the Appendix for more details. Therefore, Tracker Radar was not able to categorize PlayStation's primary CDN domains as tracking-related, which is a limitation of this type of observational testing if the third-party VR app's domains are obscured through a hosting provider, or rotate so frequently as to avoid discovery and cataloging by observability tools such as Tracker Radar.

Similarly with other large platforms, such as those hosted by Meta, Google, Amazon, Microsoft, or Apple, most, if not all, traffic goes to the same domains, meaning we may not have enough insight into what data is going where, or how it is being used once it leaves our device or network. Because of the potential lack of direct observability, we must rely on the promises device manufacturers and applications developers state in their privacy policies.

VR Risks and Harms

Parents and caregivers of children, as well as society at large, have a responsibility to look out for children's well-being. Children's brains and emotional understanding of the world around them are constantly evolving. Depending on their developmental maturity, children have vulnerabilities that change over time as they develop and mature into adults. Researchers are constantly learning new information about critical developmental stages, challenges posed, growth during specific age ranges as well as psychological, cognitive, and emotional advancements and vulnerabilities children may be particularly susceptible to within specific developmental stages.

As part of ensuring the well-being of our children, it's important to make sure children have safe spaces filled with trustworthy people and interactions that are constantly and actively considering their unique needs, health, and safety. For example, in physical spaces, such as playgrounds, adults regularly monitor who is in that physical space. At the playground, regardless of whether the adults present are also a parent, they monitor how others may be interacting or potentially interacting with kids while they are at play. Supervising kids in virtual environments is equally important. An appropriate level of understanding, care, and awareness needs to be applied to ensure healthy child development. [247] Particularly, we need to expand our tools and awareness of media rich VR experiences and environments to better protect our kids from potential risks and harms. [248]

Virtual environments create unique challenges to ensuring safe play spaces for children, and in their current form many users experience sexism, racism, homophobia, and other forms of harassment, stalking, and abuse. [249,250,251] Many of these issues require a more in depth discussion and while certainly intersectional with many aspects of privacy, they require a more in-depth analysis inclusive of users who experience these issues firsthand. As such, it is critical to ensure the platforms and content that kids engage with, and the respective communities, are age appropriate and have appropriately considered healthy child development as part of their development and continued support.

To this point in time VR, as a consumer technology, has largely been shaped and designed with gaming in mind, including their respective communities where interactions are largely unmonitored, unregulated, and codes of conduct are typically nonexistent or rarely enforced. Companies in the VR space can and should do better, human rights and dignity should not be an afterthought in product design. [252] As most of the VR devices and third-party VR apps currently on the market indicate *they are not developed or intended for kids under certain ages*, and given the little research we do have regarding children of various ages engaging with VR platforms and VR content, an additional level of caution, supervision, and reflection is a critical element of healthy engagement with VR. Just like with other media, and even more importantly with VR, it is essential to consider individual children's understanding of their experiences to determine what is appropriate for them individually and adjust media habits accordingly. However, given the additional potential risks and the subtle ways behavior can be manipulated using sensitive and real time information, additional caution in VR is warranted

Below we briefly review existing research into these issues that can help illustrate some of the privacy challenges that may require additional safeguards and precautions given that VR enables the ability "*to connect*

[247] *See* Aubrey, J.S., Robb, M.B., Bailey, J., & Bailenson, J. (2018). Virtual reality 101: What you need to know about kids and VR. *Common Sense Media*. https://www.commonsensemedia.org/sites/default/files/research/report/csm_vr101_final_under5mb.pdf.

[248] *See* Reed, N., & Joseff, K. (2022). Kids and the metaverse: What parents, policymakers, and companies need to know. *Common Sense Media*. https://www.commonsensemedia.org/sites/default/files/featured-content/files/metaverse-white-paper-1.pdf.

[249] Oremus, W. (2022, February 7). Kids are flocking to Facebook's 'metaverse.' Experts worry predators will follow. *Washington Post*. https://www.washingtonpost.com/technology/2022/02/07/facebook-metaverse-horizon-worlds-kids-safety/.

[250] *See* Bokinni, Y. (2022, April 25). A barrage of assault, racism, and rape jokes: My nightmare trip into the metaverse. *The Guardian*. https://www.theguardian.com/tv-and-radio/2022/apr/25/a-barrage-of-assault-racism-and-jokes-my-nightmare-trip-into-the-metaverse.

[251] *See* SumOfUs. (n.d.). *Metaverse: Another cesspool of toxic content*. https://www.sumofus.org/images/Metaverse_report_May_2022.pdf.

[252] Heller, B. (2020, June 12). Reimagining reality: Human rights and immersive technology. *Carr Center Discussion Paper Series*. https://carrcenter.hks.harvard.edu/publications/reimagining-reality-human-rights-and-immersive-technology.

your identity to your innermost thoughts, wants, and desires.". [253]

Humans are constantly and unconsciously broadcasting information. VR technology enables this constant broadcast and incredibly sensitive information to be captured such as: where we look, how long we look, what our pupils are doing, whether our skin is perspiring or not, as well as minute fluctuations in skin color. [254] In many cases, these automatic body responses and functions can betray our innermost thoughts and feelings that we may feel are private and are not for sharing with others without our consent. For example, researchers have also been able to use pupil dilation and eye tracking information to determine or detect a myriad of sensitive information about people including who they are sexually attracted to, whether they are likely to develop dementia, and serious ailments including schizophrenia, Parkinson's disease, ADHD, as well as concussions. [255] Our understanding of the sheer amount of insight into our cognitive and emotional state these behaviors and bioinformatics broadcast is constantly expanding.

In a landscape where misinformation and disinformation are a hugely troubling aspect of modern society, the possibility of creating false memories in VR should be treated with serious concern. [256] Researchers have explored what happens when rich forms of media similar to modern VR are used to elicit false memories. [257] They were able to elicit false memories in preschool and elementary age children that were more effective with immersive media rich environments (VR) as opposed to strictly verbal suggestions. The researchers depicted scenarios where the child either swam with orcas or shrunk to the size of a stuffed mouse and danced with the mouse. As the researchers indicate, their study "provides another interesting, innovative way to elicit false memories in children."

Researchers have also shown that media-rich VR environments create unique opportunities to influence people's behavior, including creating more favorable brand attitudes and influencing purchasing decisions. [258] Other research indicates that modern rich immersive VR environments have tremendous potential to affect human experiences and shape how we think about ourselves and our experiences in our daily lives, even when not using media in the real world. [259]

To illustrate a comparison: If the VR company or app was fully personified in the real world, would you let your kid play with that person unsupervised? The same level of consideration is certainly warranted with dynamic and interactive content that can read, respond to, and mimic [260] visual and biometric information such as pupil dilation, eyeblinks, and blushing that our kids may unconsciously be broadcasting into the world. [261] Modern advancements in AI are constantly pushing our boundaries of understanding what information may be present that we previously thought not present in an image, picture or other source of information. For instance, recent research has indicated that an algorithm can accurately predict a person's race from a particular X-ray. [262] Given the increasing level of automation and AI-driven decision-making, where models are rewarded and trained [263] to incentivize the amount of time users spend on a platform so that they spend more money, it is particularly important to reflect on monetization strategies and whether interactive media or its content creator, the platform, and/or the community that surrounds that experience is worthy of our trust. [264]

[253] *See* footnote 252.

[254] Kröger, J.L., Lutz, O.H., & Müller, F. (2020). What does your gaze reveal about you? On the privacy implications of eye tracking. *Privacy and Identity Management. Data for Better Living: AI and Privacy. Privacy and Identity 2019. IFIP Advances in Information and Communication Technology*, 576. https://doi.org/10.1007/978-3-030-42504-3_15, 228.

[255] *See* footnote 252.

[256] Bailey, J. O., Bailenson, J., Obradovic, J., & Aguiar, N. R. (2017, May). Immersive virtual reality influences children's inhibitory control and social behavior. Paper presented at the International Communication 67th Annual Conference, San Diego, CA; *See* Lombard, M., & Ditton, T. (1997). At the heart of it all: The concept of presence. *Journal of Computer-Mediated Communication*, 3(2). http://dx.doi.org/10.1111/j.1083-6101.1997.tb00072.x.

[257] Segovia, K.Y., & Bailenson, J. (2009). Virtually true: Children's acquisition of false memories in virtual reality. *Media Psychology*, 12, 371–393. https://stanfordvr.com/mm/2009/segovia-virtually-true.pdf.

[258] "By seeing the self avatar use a product and its brand, users are likely to cultivate more favorable brand attitude and purchase intention via self-endorsing than by seeing other avatars use other products and brands." Ahn, S.J.G., & Bailenson, J. (April 2014). Self-endorsed advertisements: When the self persuades the self. *The Journal of Marketing Theory and Practice*. https://doi.org/10.2753/MTP1069-6679220203.

[259] Lavoie, R., Main, K., King, C., & King, D. (2021). Virtual experience, real consequences: The potential negative emotional consequences of virtual reality gameplay. Virtual Reality, 25(1), 69–81. https://link.springer.com/article/10.1007/s10055-020-00440-y.

[260] "When the pupils of interacting partners synchronously dilate, trust is promoted, which suggests that pupil mimicry affiliates people." Prochazkova, E., Prochazkova, L., Giffin, M.R., Scholte, H.S., De Dreu, C.K.W., & Kret, M.E. (2018, July 31). Pupil mimicry promotes trust through the theory-of-mind network. *Proc Natl Acad Sci USA* 115(31). https://psycnet.apa.org/doi/10.1073/pnas.1803916115.

[261] Kret, M.E. (2015, May 27). Emotional expressions beyond facial muscle actions. A call for studying autonomic signals and their impact on social perception. *Front Psychol*. 6:711. https://doi.org/10.3389/fpsyg.2015.00711.

[262] Gordon, R. (2022, May 20). Artificial intelligence predicts patients' race from their medical images. *MIT News*. https://news.mit.edu/2022/artificial-intelligence-predicts-patients-race-from-medical-images-0520.

[263] *See* reinforcement learning, a branch of machine learning in which models are trained to encounter new or novel experiences and then exploit current knowledge in order to maximize a reward. "Reward" here is an arbitrary function, as determined by the algorithm or machine-learning model creator, that the trained model attempts to maximize.

[264] *See* Stop Hate for Profit. (2021, June 16). One year after stop hate for profit: Platforms' progress. https://www.stophateforprofit.org/platforms-progress-year-later. ("These companies' slowness, even reticence, to act boldly and at the appropriate scale guarantees that hateful content, conspiracy theories, and misinformation will keep growing relatively unabated to the detriment of all.")

Researchers have shown that people can be cued to make riskier choices.[265] Extrapolating out to AI-generated feeds, users might be encouraged to click on riskier content or to engage with content where media characters[266] that children may already have built trust relationships with may be auto-generated to encourage longer media engagement. It has already been shown that this generated, derivative, and intentionally manipulative content targeted at particularly vulnerable children happens on existing platforms.[267] Future interactions with bad actors who have access to rich, immediate biometric feedback could use this additional information to automatically craft objectionable content or encourage ideologies that parents may find objectionable, all presented in a dynamically changing format with trusted characters. The content could also be presented in such a way that a particular kid may be especially vulnerable to manipulation that would be difficult for parents or others to reproduce for reporting purposes.

Much of the above research has been demonstrated in a clinical or research setting, and it is unclear how these findings will play out in largely uncontrolled VR environments that are shifting and evolving in real time. However, given the prevalence of trolling, griefing[268], and harassment on existing VR experiences and shared gaming communities as well as research indicating that some users believe particular harassment tools are effective, it is clear that industry standards should require effective harassment mitigation design and tools.[269]

However, the work to avoid harassment should not primarily be delegated to those being harassed to do additional work to avoid harassment. The existing status quo needs to improve considerably such that targets of harassment have more clear and effective ways to avoid harassment, preferably before it even happens. Even content that does not have social features or functionality where users interact with other VR users, such as solo VR gaming, should take into consideration what normative behaviors they are encouraging as the skills developed and experiences will carry over into other VR environments. Existing user experience implies that companies are likely losing out on additional revenue. If they continue to permit harassment on their platforms, users' only option to avoid harassment may be to not participate. VR apps and games typically invest resources in either a single player or multiplayer experience as their primary source of revenue but often rely on secondary revenue streams, including microtransactions, to create a virtual economy. This includes in-app purchases for virtual goods, or additional expansion content that can create billions of dollars in revenue.[270] These types of microtransactions are often difficult for kids and adults to distinguish play money versus real money and it is not always apparent what things cost in real money terms. Younger kids and teens also want to make people happy, and they don't want to disappoint their friends, or their family, and this also includes their favorite virtual characters who may ask them to make purchases.[271] Additionally, there are concerns with respect to gambling and other problematic behavior. In addition to financial and potential gambling issues, in app or in game cosmetics may result in bullying where kids feel peer-pressured to spend more time or money in game to avoid ridicule among their peers.[272]

Privacy and control over user privacy is an important element of improving these spaces as giving users more autonomy and control over their virtual representations and experiences can set the stage for what types of interactions and experiences are even possible.[273] This is an evolving space that will require ongoing research and consideration to ensure the spaces we create and the communities we build are a net positive and not a detriment to society. A necessary first step to ensuring we are able to improve these spaces and hold companies accountable is more transparency about how data is collected, used, and shared as well as clear transparency regarding user experiences.

[265] Cherkasova, M.V., Clark, L., Barton J.J.S., Schulzer, M., Shafiee, M., Kingstone, A., Stoessl, A.J., Winstanley, C.A. (2018, November 28). Win-concurrent sensory cues can promote riskier choice. *J Neurosci* 38(48): 10362–10370. https://doi.org/10.1523/JNEUROSCI.1171-18.2018.

[266] "Media characters serve as social partners and friends who can garner trust, thereby influencing both cognitive and social development." Aguiar, N.R., Richards, M.N., & Calvert, S.L. (2018, November 12). Children's parasocial breakups with media characters from the perspective of the parent. *Imagination, Cognition, and Personality* 38(3), pp. 193–220. https://doi.org/10.1177/0276236618809902.

[267] Common Sense Media. (2013). *Media and violence: An analysis of current research*. https://www.commonsensemedia.org/sites/default/files/research/report/media-and-violence-research-brief-2013.pdf. *See also* the TED Talk video "The nightmare videos of children's YouTube—and what's wrong with the internet today." https://www.ted.com/talks/james_bridle_the_nightmare_videos_of_children_s_youtube_and_what_s_wrong_with_the_internet_today.

[268] "Intentional harassment of other players is called 'griefing,' which utilizes aspects of the game structure or physics in unintended ways to cause distress for other players." Warner, D.E., & Raiter, M. (2005). Social context in massively-multiplayer online games (MMOGs): Ethical questions in shared space. *International Review of Information Ethics*. http://www.i-r-i-e.net/inhalt/004/Warner-Raiter.pdf.

[269] Pluto VR and the Extended Mind. (2018). *The extended mind: Survey of social VR users*. https://www.extendedmind.io/2018-survey-of-social-vr-users.

[270] *See* the FTC's "Inside the Game: Unlocking the Consumer Issues Surrounding Loot Boxes." https://www.ftc.gov/news-events/events/2019/08/inside-game-unlocking-consumer-issues-surrounding-loot-boxes.

[271] "There are other children's games in which a character will cry if the child doesn't make the purchases recommended. I think it bears noting here that host selling like this is prohibited on TV. And here you have not only the host selling, but the host getting angry or upset with a child if they're not making a purchase immediately." https://www.ftc.gov/system/files/documents/public_events/1511966/loot_boxes_workshop_transcript.pdf.

[272] Hernandez, P. (2019, May 9). Fortnite is free, but kids are getting bullied into spending money. *Polygon*. https://www.polygon.com/2019/5/7/18534431/fortnite-rare-default-skins-bullying-harassment.

[273] McGill, M. (2021). Extended reality (XR) and the erosion of anonymity and privacy. The IEEE Global Initiative on Ethics of Extended Reality. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9619999.

Conclusion

There's a beginning to the VR story where our superhero and villain origins are explained, and then we understand why they act the way they do, and why they have such power over us. We're past that moment now, and entering a new chapter where we are likely to spend an increasing amount of time living in their world. If we allow our children to "live" in the metaverse, we need to apply the same standards of protection that we would for any neighborhood. We will need to know who else is there with us, and whether they are responsible users and can be trusted. We will also need to know how we can protect our privacy and safety in this new reality.

While we hypothesize that new forms of monetization of users' data will eventually materialize as VR continues to develop, we also propose several potential solutions. There should be more privacy settings for VR applications to restrict sensitive data collection and impose data minimization for first-party *and* third-party applications. VR devices should include permission settings related to the usage of user data for 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 that are potentially far more invasive and exploitative than any other form of advertising known to date.

The below sections describe what each stakeholder can do, in the process of protecting privacy in the VR industry, to make the risks lower and the benefits higher for users of these products and services. Policymakers, parents and educators, developers, and other users must all step up to take action to improve this VR ecosystem. It's not an all-or-nothing scenario, and each action makes a difference.

What should policymakers and regulators do?

Legislators and regulators are uniquely poised to take action to protect vulnerable users in the emerging virtual reality space.[274] Several policy analysts have also offered suggestions for how to effectuate these policies,[275] including supervising children's use of the technology. Policymakers should also consider new forms of legislation that apply to the increasing amount of sensitive personal information collected by virtual reality devices and applications, which, as shown by this report, are exploiting users' virtual reality experiences, behavior, safety, and personal information for profit.[276] The following policy recommendations should apply to all virtual reality device manufacturers and software application developers:

- **Enforcement of false and misleading privacy information**. Just as we regulate our food system to protect the public's health and the safety of food products, we also need to urgently protect the privacy of consumers, kids, and families in the metaverse. This report indicates that across the app stores, VR devices and third-party VR apps that are targeted or would appeal to kids, teens, and students have worse privacy practices that put users at risk. Many companies also are nontransparent in their policies about how they protect users' data in VR. Additionally, VR device manufacturers and third-party VR apps may use false and misleading advertising in the VR app stores, claiming they "care about your privacy" but engaging in numerous worse privacy practices in order to encourage the purchase of VR devices and increase the number of VR app downloads. Strong enforcement of false and misleading advertising in the metaverse as it evolves would incentivize companies to tell the truth about their privacy practices from the beginning, which ultimately helps consumers make better-informed and safer choices for themselves and their families.
- **Prohibit behavioral manipulation**. Using any of a user's biometric, sensitive, or personal information collected in virtual reality for exploitive or persuasive commercial purposes should be prohibited. New forms of monetary value in VR could expose users to manipulation through microtransactions,

[274] Congressional Research Service. (August 26, 2022). The Metaverse: Concepts and Issues for Congress, https://crsreports.congress.gov/product/pdf/R/R47224.

[275] *See*, e.g., Letter to United States Senator Markey, https://www.markey.senate.gov/imo/media/doc/letter_to_ftc_-_vr_and_children.pdf.

[276] *See* footnote 248.

NFTs,[277] in-app tokens (like Zuck Bucks,[278]) or cryptocurrency. These forms of virtual currency and microtransactions should be scrutinized as part of the new, unregulated virtual creative economy in the metaverse. Behavioral data collected from users in virtual reality is so highly sensitive and personalized that it should be off-limits and never used to influence or change a user's behavior, interactions, or decision-making in virtual reality or elsewhere, whether for profit, ideological, or political reasons.

- **Prohibit tracking**. A user's virtual reality device or experiences in a virtual reality application should not be tracked across the internet or on other devices or applications outside VR for commercial purposes. What happens in virtual reality should stay in virtual reality.
- **Prohibit targeted advertising**. A user's virtual reality experiences and data collected from their use of virtual reality devices should not be used for targeted advertising. A user's virtual reality experiences, behaviors, preferences, and interactions should not be monetized by companies for commercial purposes.
- **Prohibit use of anonymized data**. Any de-identified or anonymized data, or even data from a pseudonym collected from users or bystanders in virtual reality, should not be shared with third parties or used without prior institutional review board (IRB) authorization and written informed consent from users. The use of virtual reality applications and devices should not force users to become unwilling research subjects without their knowledge and explicit informed consent.
- **Prohibit unrestricted sharing**. A user's data in virtual reality should not be shared with any third parties, affiliates, or partner companies for any other purpose, except as necessary to provide the service. Virtual reality experiences and the sensitive data collected from users should not be treated as a commodity to share with a company's business partners for their own purposes.
- **Prohibit the sale of user data**. A user's data should not be sold or rented to third parties without their explicit opt-in consent. Privacy in virtual reality should be the default, and should not require users to jump through multiple hoops to opt out of the sale of their data.
- **Prohibit transfer of user data**. A user's data should not transfer ownership to third parties in the event of a company merger, acquisition, or bankruptcy without explicit opt-in consent. Data in virtual reality should not be treated as an asset that can be monetized by companies looking for a quick return on their investment or exit strategy from the marketplace.

What should parents and educators do?

Parents, caregivers, and educators have several options when deciding whether to use virtual reality apps and devices. Some may be thinking about which virtual reality device they should purchase, and others may have already made up their mind but aren't sure if it's best for privacy. Some may want to know how to change their virtual reality device's privacy settings to best protect themselves and their teens or students. Parents and educators also may want to know how to exercise their data rights and tell companies not to sell their data for profit. Below are some suggestions for parents and educators to better protect the privacy of their children and students:

- **Check the privacy settings**. All virtual reality devices have some settings that allow varying degrees of data collection features, advertising, or marketing communications to be turned on or off. For example, if it's not necessary to collect hand tracking, voice data, or analytics data on how the device is used, then these extra features can be turned off to minimize the amount of sensitive information collected and used for purposes beyond those the user intended.
- **Check the safety settings**. Some virtual reality devices and applications have software safety features that can limit what profile information is publicly shared with others and who can contact the user. For example, it's best practice to start with the most privacy-protecting settings by default, such as limiting who can see a user's online status or letting a user chat only with trusted friends and family.
- **Check Common Sense Media**. Virtual reality applications may not be age appropriate, or may engage in worse privacy practices that can put children or students at risk. The Common Sense Privacy Program evaluates the privacy policies of popular consumer technology applications and services, like VR, that are currently used by millions of children at home and in the classroom. Child-related applications and services used at home include a wide range of technologies, such as games and apps for communication, collaboration with friends, content creation, and delivery of media entertainment. Parents and caregivers can use our easy-to-understand privacy evaluations to make informed choices about the products they use at home, and

[277] A non-fungible token (NFT) could enable metaverse users to record ownership of digital assets purchased within the metaverse. The user could control, trade, store, and use their NFTs across VR apps in the metaverse. The ownership of a user's NFT is recorded on the blockchain network and represents a value on the decentralized finance (DeFi) market. Metaverse NFTs can be traded for digital assets, such as Bitcoin (BTC) or Ethereum (ETH), on supported NFT marketplaces and decentralized exchanges (DEXs).

[278] *See* Murphy, M. (2022, April 6). Facebook owner Meta targets finance with 'Zuck Bucks' and creator coins. *Financial Times*. https://www.ft.com/content/50fbe9ba-32c8-4caf-a34e-234031019371.

pass that information on to other families who use the same apps with their kids. Helpful summaries show how companies address safety, security, privacy, and compliance in their policies and terms of service. Privacy evaluations speed up the decision-making process so parents can find the most appropriate apps to use with their children at home and in their daily lives.[279]

In addition to better legislation and platform accountability, consumer education, awareness, and behavior with privacy are important elements in improving online communities or knowing when a community is unhealthy for one's own self, and this is even more critical in VR environments. Common Sense's Digital Citizenship Curriculum can also educate parents, educators, children, and students about these important issues.[280]

- **Encourage supervision**. Children and students should not use virtual reality devices, games, or apps if they are younger than 13 because the long-term effects of VR use on their developing brains and possible future privacy concerns are still unknown.[281] 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. Parents and educators may also be able to encourage teens and students to limit the types of personal information they provide to virtual reality devices and applications, both before and during the use of VR.
- **Check which apps are installed**. Remove unwanted or unused virtual reality software on personal computers, and remove third-party virtual reality apps from virtual reality devices to limit personal information collection from other companies.
- **Ask companies not to sell your data**. Use free online resources, like donotsell.org,[282] to request that companies not sell your personal data collected in virtual reality for profit.
- **Turn off internet connectivity**. In some limited cases, turning off internet access on the VR device may limit the real-time sharing of a user's sensitive data collected through a VR app with the company or other third-party companies. However, many first-party and third-party VR apps require a user to be connected to the internet in order to function properly and will not load otherwise. Also, apps may simply cache or store a user's sensitive data on the device if collected offline, and as soon as the VR device later connects to the internet, the previously stored data is shared with third parties.
- **Wipe devices before resale**. By design, VR devices require users to log in with their account and register their device with the manufacturer or other companion software or app stores. However, upon first use of the VR device, some users may experience motion sickness, dizziness, or eye strain if they have never used these types of devices before. Other users may simply decide they are not interested in VR. If parents choose to resell or give away their recently purchased VR device, they need to remember to delete all accounts and unregister the device with the manufacturer. It's also important to remove any personal information on the device, just like wiping all of your data off a smartphone before trading it in.
- **Make your preferences known to companies and legislators**. Many parents have taken (or wanted to take) steps to limit data collection—recent research indicates about half of those surveyed think they have taken such steps, and half want to but don't know how.[283] This is the jumping-off point for action. The next step is to empower parents and educators so that they know how to exercise their privacy-protecting options. Parents can vote with their dollars and feet by telling companies they won't buy their VR devices or VR apps if they don't have better privacy. Parents can also contact their state and local representatives about their concern for stronger privacy, or join Common Sense advocacy campaigns to participate in our collective action fighting for stronger privacy laws.[284] Legislators can support their constituents by mandating that sensitive VR data is off-limits and not for sale, and when that doesn't fully protect users, allowing a private right of action for individuals to enforce the law.
- **Make informed decisions about which apps to use**. This report is a snapshot of virtual reality apps and devices right now. Business practices change rapidly as companies think creatively about how to gather, process, and sell data collected from users in virtual reality. In deciding whether to purchase a virtual reality device or use virtual reality apps, consider the impact on children and students who will use the device and the amount of virtual reality screen time they will spend. Factor into your decision the cost of the device, as well as software purchases that may be made for other virtual reality apps or games, and the potential use of your personal information by the company and other

[279] *See* Common Sense Privacy Program: https://privacy.commonsense.org.

[280] *See* Common Sense Education Digital Citizenship Curriculum: https://www.commonsense.org/education/digital-citizenship.

[281] *See* footnote 247.

[282] CCPA: Do Not Sell My Information, http://donotsell.org.

[283] Parents may be only marginally aware of the pervasiveness of child use of VR, and the risks. *See* Reed, N., & Joseff, K. (2022). Kids and the metaverse: What parents, policymakers, and companies need to know. *Common Sense Media*. https://www.commonsensemedia.org/sites/default/files/featured-content/files/metaverse-white-paper-1.pdf.

[284] *See* Common Sense Advocacy: https://www.commonsensemedia.org/kids-action.

third-party companies that might monetize your or your kids' data over time.

What should developers and manufacturers do?

We encourage virtual reality developers and manufacturers to view the findings in this report as a baseline of the state of virtual reality privacy today, and to increase the transparency and quality of their privacy practices as part of their ongoing process of product improvement. There is a growing awareness of privacy in the marketplace, and a need for developers and manufacturers to differentiate their applications and services from the industry at large. Currently, there are no popular virtual reality devices available that differentiate themselves by having better privacy-protective practices. However, parents, educators, and consumers are actively looking for VR manufacturers and developers to fill that gap and may be more likely to purchase virtual reality headsets and applications that protect their privacy. Below are some suggestions[285] for virtual reality developers and manufacturers to better protect their users' privacy:

- **Age-gates and profiles**. Consider establishing age controls to verify actual knowledge or use constructive knowledge to prevent account setup and use by children under 13 years old, and to identify teen users older than 13 but younger than 18.[286] Additionally, companies may also want to establish reverse age gating to prevent adults 18 and older from self-identifying as children or teen avatars when engaging in social communication. This gets complicated when the interactions are not text profiles but avatars that appear young, or that use voice-altering applications to make an adult's voice sound like a child's. However, providing voice-masking privacy controls by default can protect kids' safety and preserve their anonymity in public spaces.[287]
- **Create safe spaces**. Develop separate applications or separate "walled garden" areas of existing applications that only allow adults, children, or teens with parental consent to interact safely among their peers. Create activities and use options that appeal to different age-band audiences and segments of the population.
- **Limit screen time**. While screen time limitations, or at least notifications of time elapsed, may be useful to adult users, consider requiring a hard stop after a certain amount of time or at a certain hour for children under 13 to prevent screen addiction, sleep deprivation, poor school performance, and other negative outcomes associated with overuse and overstimulation, such as confusion or eyestrain.[288]
- **Limit data retention**. Consider the benefits of data erasure after a certain period of time has elapsed, regardless of whether the user has deleted their account. Options include deleting a profile and/or session usage data after exiting the application, or within 24 hours of exiting.
- **Presume anonymous users are children or teens**. Assume all anonymous users are under 18, and may also be younger than 13. Limit the collection of personal information from all anonymous users, and limit their ability to enter personally identifiable data or interact with other anonymous users to make sure children and students are not inadvertently exposed to worse privacy practices by default.
- **Promote more diversity in the workforce**. Many issues related to privacy play out disproportionately for specific communities. Some potential risks and harms could be avoided, or certainly minimized, by having a more diverse workforce, especially in decision-making, leadership, and technical roles. When a large portion of historically underrepresented people experience discrimination, harassment, and microagressions in the worklplace, is it reasonable to expect that companies can create products, environments, and communities that don't perpetuate the same issues?[289]
- **VR privacy and security by design**. Have all privacy and safety settings for the device or third-party application set by default to provide the most privacy-protecting settings possible[290] for the user, and give them the agency and choice to make an informed decision to change those settings to reduce their privacy or safety expectations. Security by design is also important, and end-to-end

[285] *See* previous VR-specific privacy-enhancing suggestions for developers from Common Sense Media available at https://www.commonsensemedia.org/sites/default/files/featured-content/files/safe_and_secure_vr_policy_issues_impacting_kids_final.pdf , pp. 2–3.

[286] We know that younger children are using the devices, even if the policies proclaim that they are not supposed to use the product, or are allowed to use it only with adult supervision. For example, "Jeff Haynes, senior video games editor for the nonprofit Common Sense Media, which reviews entertainment with an eye to age appropriateness, said he has found the pervasiveness of kids in Horizon Worlds 'alarming,' encountering youngsters 10 and younger every time he has used it." https://www.washingtonpost.com/technology/2022/02/07/facebook-metaverse-horizon-worlds-kids-safety/.

[287] *See* footnote 162.

[288] Bailenson, J. (2018, January 17). Eight rules to help you stay safe in virtual reality. *Slate*. https://slate.com/technology/2018/01/eight-rules-to-help-you-stay-safe-in-virtualreality.html.

[289] *See* Funk, C., & Parker, K. (2018, January 9). Women and men in STEM often at odds over workplace equity. *Pew Research Center*. https://www.pewresearch.org/social-trends/2018/01/09/women-and-men-in-stem-often-at-odds-over-workplace-equity.

[290] General data protection and privacy principles apply in XR as elsewhere, including data minimization, anonymization, encryption, and localization of data. *See* Jerome, J., & Greenberg, J. (2021, April). Augmented reality + virtual reality: Privacy & autonomy considerations in emerging, immersive digital worlds, pp. 28. The Future of Privacy Forum. https://fpf.org/wp-content/uploads/2021/04/FPF-ARVR-Report-4.16.21-Digital.pdf.

encryption[291] of all communications and content should be the default.

- **Industry-wide community standards**. Industry standards have worked in other tech industries, and serve to augment or even replace the need for regulation if they are universally adopted.[292] Standards may involve content moderation,[293] including appropriate VR experiences and content for children, as well as consequences for violating industry standards for different populations. A single company can take the lead, or an industry-wide consortium can create a code of conduct for interaction in the VR space. Interoperability can facilitate these standards, as in order to move seamlessly from one VR space to another, technical standards need to be developed and user behavior should be relatively similar in each space.[294] Setting these expectations will encourage adoption and use of XR technology for a variety of purposes.

[291] Visual encryption in VR described in Zhao, et. al, "VR in Metaverse: Security and Privacy Concerns," available at https://arxiv.org/pdf/2203.03854.pdf.

[292] *See*, e.g., Oasis's "User Safety Standards," for a start, at https://www.technologyreview.com/2022/01/20/1043843/safe-metaverse-oasis-consortium-roblox-meta/.

[293] For a discussion of content moderation to avoid privacy risks and harms, see Heller, B., & Bar-Zeev, A. (October 2021). The problems with immersive advertising: In AR/VR, nobody knows you are an ad, pp. 11. *Journal of Online Trust and Safety*. https://tsjournal.org/index.php/jots/article/view/21/10.

[294] Cyphers, B., & Doctorow, C. (2021, February 12). Privacy without monopoly: Data protection and interoperability. *Electronic Frontier Foundation*. https://www.eff.org/wp/interoperability-and-privacy.

Appendix

Methodology

To perform basic information security testing, we created a "blank slate" testing environment that monitored only the data sent and received between a virtual device, its companion mobile application (if applicable), personal computer, and the internet.[295] This included purchasing and setting up networking hardware equipment to monitor network traffic in order to create a specific type of testing environment. Also, iOS[296] and Android[297] mobile devices were used for testing. Each were factory reset without any personal information loaded onto the device in order to test only a single companion mobile application at a time. Additionally, software was installed on a separate local testing computer for network packet analysis.[298]

Several different types of information security testing could be used to monitor network traffic and determine security vulnerabilities of VR devices. Some methods make extensive use of an intercepting software proxy to observe, and in some cases modify, encrypted network requests generated by the application.[299] There are also mobile application frameworks that can be used with Android mobile devices or Virtual Private Network (VPN) apps on iOS devices to observe network requests from a mobile application to the internet. However, these advanced approaches are still limited for the purposes of our basic security testing because they can observe 1) decrypted network traffic between the mobile application and the internet, and 2) decrypted network traffic between the virtual reality device and the personal computer or mobile device, but they cannot decrypt and observe data sent from the VR device directly to the internet.[300]

When researching which method to use for our basic information security testing, we considered how difficult it would be for nontechnical educators and students to reproduce our network testing environment for their own educational and testing purposes.[301] Therefore, we designed our method of basic information security testing to be used as part of a project-based collaborative development experience for both teachers and secondary students to increase their experience with and knowledge of hands-on software and hardware tools and how to test the privacy and security of a mobile application, online service, or VR device. Through the unifying theme of learning about new and emerging technologies such as VR, teachers and students could work together to learn about various technologies (focusing on their individual interests and use of the technology). It's also possible to use this process to consider how to protect their privacy and gauge the security of their data while engaging with everyday technologies, like virtual reality devices.

We believe the following testing process that uses a hardware-based network environment testing approach with the preconfigured open-source data analysis software Security Onion is the easiest method to set up and start security testing VR devices quickly with educators and students.[302] Security Onion software provides an out-of-the-box solution that is easy to install on a computer and provides extensive documentation for educators and students to learn how to perform basic network security analysis.[303]

In addition, Security Onion software also provides the flexibility for more advanced security testing for students if desired using the open-source Linux operating system.[304] Security Onion can also be installed in a virtual machine,[305] which allows students and researchers without access to the VR devices to reproduce our testing results and investigate the findings themselves by importing the original pcap (packet capture of network traffic) data used for testing.

Overall, the goal of designing the testing environment was to get educators and students to start testing the privacy and security of VR devices with minimal effort

[295] Ren, J., Dubois, D.J., Choffnes, D., Mandalari, A.M., Kolcun, R., & Haddadi, H. (October 2019). Information exposure from consumer IoT devices: A multidimensional, network-informed measurement approach, pp. 267–279. *IMC '19: Proceedings of the Internet Measurement Conference*. https://doi.org/10.1145/3355369.3355577.

[296] iOS is a mobile operating system created and developed by Apple Inc. for iPhone.

[297] Android is an open-source operating system used for smartphones and tablets.

[298] *See* OWASP Zed Attack Proxy (ZAP): https://www.zaproxy.org/.

[299] Intercepting proxies are tools used to analyze the normal session created between a client and server.

[300] *See* footnote 53.

[301] While some of the audience for our research may be technologists, academics, or IT professionals, we also seek to inform district technology coordinators and classroom teachers who may have no technical background.

[302] *See* Security Onion: https://securityonion.net/.

[303] *See* Security Onion Documentation: https://securityonion.readthedocs.io/en/latest/.

[304] Linux is a family of open-source Unix-like operating systems based on the Linux kernel.

[305] *See* Oracle VM VirtualBox: https://www.virtualbox.org.

and a small learning curve. Therefore, we believe the following network testing environment relies more on a basic hands-on networking approach with the use of basic operating system installation skills, rather than extensive computer science knowledge of open-source software tools and Unix administration processes [306] often used by security professionals to configure information security testing environments.

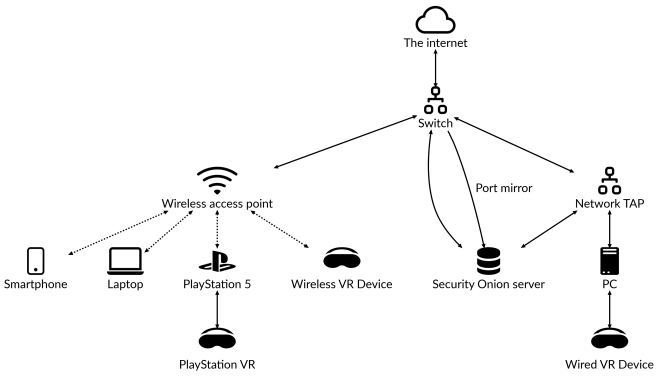
Network testing environment

The diagram below illustrates the basic network topography environment used for testing all seven virtual reality devices. However, it is important to note that every network hardware configuration is different and may require different devices to connect to the internet, such as a DSL [307] or cable modem, router, or gateway, that may need to be configured to allow the network switch in our diagram below to connect to the internet.

There are two network testing configurations explored for testing VR devices: 1) wired connection using a network tap, and 2) wireless connection using a network switch port mirror. A wired testing environment is preferred when the VR device connects directly to a personal computer which then connects to the internet using a wired ethernet cable. The PlayStation VR was wired directly to the PlayStation 5 console. In addition, the HP Reverb G2, HTC Vive Cosmos Elite, Valve Index, and Pimax Vision 5K Super VR devices were all connected to the personal computer (PC).

A wireless testing environment is preferred when the VR device connects directly to the internet wirelessly through a wireless access point. The Microsoft HoloLens 2, and Meta Quest 2 VR devices wirelessly connected to the Wireless Access Point (WAP).

Figure 8: Image of network testing environment structure



The following sections describe the components required for the testing environment:

The internet The basic information security testing environment requires that all devices be connected to the internet in order to make and receive network requests that can be captured and analyzed by the Security Onion server. This type of security testing environment attempts to recreate as closely as possible the real-world interaction, data collection, and use of virtual reality devices and any companion mobile applications running on a smartphone.

Network switch or network tap The switch in our testing environment can be a low-cost device used to connect a wireless access point to the internet and also connect a Security Onion server for monitoring all network packets received by the wireless access point. [308] In order to monitor all the network packets that are sent and received from a virtual reality device to the internet, our testing environment used a switch with port mirroring. [309] However, a network tap can also be used, which is a simple-to-use hardware device that plugs in between a wired ethernet connection and the switch, and can be used to duplicate network traffic for analysis by Security Onion. [310]

Security Onion server Security Onion is a free and open-source Linux distribution for intrusion detection, enterprise security monitoring, and log management. [311] The software is available in a downloadable image that can be used to create a bootable USB device that allows users to quickly install the network monitoring server on a personal computer that meets the sufficient hardware requirements. The Security Onion server captures network traffic [312] from the wireless access point [313] on the mirrored port of the network switch for security analysis.

Wireless access point The wireless access point in our testing environment can be a low-cost device to connect wireless devices for basic information security testing to the network switch and the internet. This network configuration allows for the network switch to mirror

[306] Unix is an operating system that supports multitasking and multi-user functionality.

[307] A digital subscriber line (DSL) is a technology that connects a computer or router to a telephone line that provides connection to the internet.

[308] A network switch is a networking hardware device that connects other devices on a computer network by using packet switching technology to receive and forward data from the source device to the destination device.

[309] Port mirroring is used on a network switch to send a copy of all network packets received on a designated switch port to a network monitoring connection on another switch port. This is commonly used for network devices that require monitoring or network traffic, such as an intrusion detection system (IDS).

[310] A network tap is a hardware device that provides a way to duplicate network data flowing across a computer network for inspection.

[311] Security Onion's name refers to the practice of peeling back layers to see more detail, as with other open-source tools like TOR (The Onion Router).

[312] Network traffic is the data set for this testing methodology. It is the flow of data from inside the product to the outside world.

[313] *See* infra Wireless Access Point. A wireless access point (WAP) is a networking hardware device that allows other Wi-Fi enabled wireless devices to connect to a wired network to gain access to network resources and/or the Internet.

all network packets[314] from the wireless access point that uses WiFi to another port on the network switch for packet capture and analysis by the connected Security Onion server.

Virtual reality device Each virtual reality device used for testing was observed either through a wired connection to the personal computer, or wirelessly connected to the wireless access point only one at a time. This ensures data captured originated from a specific device because the network tap or network switch will mirror all network traffic from the virtual reality device to another port on the network switch for the Security Onion server to capture for analysis of that specific VR device.

Personal computer A wired virtual reality device is required to be connected to a personal computer with a USB interface for data and also requires an HDMI or DisplayPort interface on the computer's graphics card to display the virtual content. Virtual reality devices require powerful graphics cards from manufacturers such as AMD or Nvidia. The personal computer used for testing was intended to be a "clean" environment with minimal installation of only Microsoft Windows 10, Nvidia graphics card drivers and software, and Steam. The personal computer was connected to the local network though gigabit ethernet and the network tap mirrored all network traffic from the personal computer to the Security Onion server to capture for analysis.

Smartphone A low-cost Android or iOS smartphone can be used in the testing environment with the mobile application used to control the virtual reality device installed. The mobile device was "factory reset" before use, meaning that the operating system had been reinstalled and no other applications were installed on the device to avoid inadvertent data collection during our basic information security testing. The mobile device was wirelessly connected to the wireless access point and the network switch mirrored all network traffic from the mobile application on the smartphone to another port on the network switch for the Security Onion server to capture for analysis.

Laptop A low-cost laptop in our testing environment was used to connect to the local area network that is connected to the wireless access point and access the basic information security testing tools on the Security Onion Server through a web browser or over an SSH terminal session.[315]

[314] A packet is a unit of data that is routed between an origin and a destination on the internet or any other packet-switched network.

[315] Secure shell (SSH) is a cryptographic network protocol for operating network services securely through terminal emulation software.

Process overview

The basic information security testing process was designed into three modules to analyze several different security-related data points with Security Onion to determine the security practices of the VR device and companion mobile application.

1. *What type of network requests are being sent and received from the virtual reality device and the mobile application?* This module illustrates what type of secure or unsecure requests are sent from the VR device to the internet and requests received between the VR device and mobile application. This analysis provides users with more information about whether reasonable security practices, such as encryption, are used to protect personal data while in transit from its source to its destination.
2. *To what destinations are network requests sent?* This module illustrates what third-party companies send and receive data from a VR device and mobile application. Intuitively, most VR devices and mobile applications communicate primarily with the manufacturer's online web services, but often third-party advertising or tracking services can be seen sending or receiving data from the VR device or mobile application.
3. *How much data is shared with the company or third parties?* This module illustrates the total amount of bytes sent from the VR device or mobile application to the company's servers or third parties. This analysis provides users with more information about when data is collected and how much data is actually collected.

This three-step modular process is helpful to illuminate who the VR device and mobile application are talking to (the company or third-party servers), but is limited because it does not show the content of the data that is actually being sent between the parties because it is likely encrypted.

Security Onion software

After the network testing environment is deployed successfully, and the virtual reality device, mobile device, and laptops can access the internet through the wireless access point, then users need to install Security Onion on a personal computer or laptop attached to the network switch. After installation of the Security Onion server, users can use their laptops to connect to the Security Onion server and begin the information testing modules that teach basic security monitoring skills. It includes preconfigured network security testing software applications and utilities, such as Elasticsearch, Logstash, Kibana, Snort, Suricata, Zeek, Wazuh, Sguil, Squert, CyberChef, NetworkMiner, and many other security analysis tools.[316]

[316] *See* Elasticsearch, https://www.elastic.co/; Logstash, https://www.elastic.co/logstash; Kibana,

Testing limitations

However, there are limitations with this basic information testing approach. Our testing results are simply a snapshot of behavior we observed from a VR device and mobile application on a specific date and time in our particular network environment, and those observations which could change based on different testing configurations or real world use. [317] In addition, firmware updates to the VR device and software updates to the companion mobile application could also change expected observational behavior from what was observed during our testing period. [318] Additionally, due to the nature of a shared environment between an app or game and a particular piece of hardware, some of the traffic will be impossible to determine if the communications were initiated by the hardware and its respective firmware and software or by the particular app or game being used at that moment. We have done our best to capture narrow windows of traffic while we were specifically interacting with a single app or game, but inevitably some of that traffic will have been initiated by the device so total experience and observed behavior should be interpreted with some caution regarding what conclusions we can say with certainty..

Our testing can only see what data is transferred from one device or server to another, but not the particular destinations on those servers, as we did not do deep packet inspection since much of the observed traffic was encrypted end-to-end and we did not make any effort to circumvent this encryption in order to observe the details. In addition we cannot observe subsequent server-to-server data processing or sharing with third parties. [319] For example, a VR device or mobile app may only send and receive data to one destination server address such as Microsoft's or PlayStation's Content Delivery Network (CDN) before forwarding the data packets off to other third-party domains to be processed elsewhere. Users will be unable to observe what the first-party company (i.e., Microsoft or PlayStation in this example) actually does with the personal information it collects after it has received it. Therefore, we believe reading the privacy policies of VR devices is also a critically important part of evaluating the privacy and security of a virtual reality device.

In addition to observing the VR device's data collection and sharing practices, it is important to know how each company promises it will process personal data after it has been collected. Combining some knowledge of actual data flows, as we have done in this testing, with the legal obligations described in the privacy policies puts more of the crucial puzzle pieces on the table. Putting them together into a coherent whole, however, requires more work.

Traffic analysis methodology

During the operation of each VR device or app, traffic was captured and later analyzed. Due to the majority of, but not all, traffic being transmitted over secure communication channels, we only have aggregate domain level information and therefore do not have insight into particular resources accessed. Each application's traffic was observed using only the lowest price point, and therefore there may be observable differences in traffic, based on different subscription models that we did not make an effort to observe. As such, any of the following analysis should be interpreted with some caution.

Our analysis is intended to indicate the possibility that the respective tracking behavior could be happening based on the VR device or app accessing resources on a particular domain known to have exhibited tracking behavior. If a domain is indicated as potentially engaging in a tracking behavior, it should be interpreted to mean that caution is warranted with respect to tracking concerns. In addition, the observed traffic does not necessarily mean that the respective tracking behavior was necessarily engaged in.

For each domain we observed, we also indicate the "Match Domain," showing which Tracker Radar domain file was used to provide the tracking categories. We only considered domains in the U.S. directory for Tracker Radar. If a domain indicates "NA," that means we did not have a corresponding Tracker Radar domain file to classify the domain traffic. Some of these unknown domains are expected as the process to obtain the Tracker Radar data is from a web browser—a context notably different than the apps or devices that we tested. As such, there may not have been opportunities for the Tracker Radar project to observe traffic as seen when using an app or device as opposed to a web browser.

We used a git checkout of the tracker-radar project with git tag '2022.06' corresponding to a git hash 757b93bc368c0a6ee6e03f14a28b179b028d3fd6.

https://www.elastic.co/kibana; Snort, https://www.snort.org/; Suricata, https://suricata-ids.org/; Zeek, https://zeek.org/; Wazuh, https://wazuh.com/; Squil, https://bammv.github.io/sguil/index.html; Squert, https://github.com/int13h/squert; CyberChef, https://gchq.github.io/CyberChef/; NetworkMiner, https://www.netresec.com/index.ashx?page=NetworkMiner.

[317] Date and time for research, or a span of time, like "January 2020."

[318] Firmware is data that is stored on a hardware device that provides instructions on how that device should operate. Firmware updates are one of the weak points in IoT security, particularly where the devices are either not updated at all and considered disposable once the initial software has become outdated, or require the user to locate and perform manual updates. In contrast to firmware updates and their security limitations, software updates may be effectuated automatically from the server, without user input, or with user input but with the click of a button.

[319] The term "third parties" is somewhat misleading in the sense that it implies that only one entity might receive the data, and in a single transaction. In actuality, data brokers and other initial recipients of the data often forward and resell this information over multiple transactions, combine data with other data for use and sale, and store data for future use and sale.

Tracking categories

For the purposes of our analysis, we only considered Tracker Radar categories[320] that could pose a privacy risk, especially because it is unlikely that a user of a VR app or device would know any tracking was happening. As such, we have excluded the "Social–Comment" and "Social–Share" Tracker Radar categories in our analysis as it is likely the user would see the respective interfaces or social share buttons making it more explicit that data is being shared or transmitted that could be used to track behavior. It should also be noted that we considered "Obscure Ownership," "Session Replay," and "Unknown High-Risk Behavior" but at least for the traffic that we were able to observe no VR devices or apps contacted domains triggering any of those Tracker Radar categories. Several other innocuous categories were also excluded. The categories we included in our analysis are as follows:

- Action Pixels (AP): This tracker may be collecting user specific events in a first-party or third-party environment.
- Ad Fraud (AF): The tracker is intended to help prevent ad fraud (either on behalf of the publisher or the network). These can come from a network (like Google) or ad middleware (software designed to identify bots and not show them ads).
- Ad Motivated Tracking (AMT): The tracking that takes place is related to advertising. This could include targeting users, header bidding, ad beacons, demographic collection, preventing ad fraud, etc.
- Advertising (AD): The purpose of this tracker is related to advertising.
- Audience Measurement (AM): Similar to analytics, but may focus on deeper demographics, behavior sets, and specific actions.
- Social Network (SN): The domain is owned by a major social network.
- Third-Party Analytics Marketing (TPAM): Related to third-party analytics systems for marketing, usually marketing attribution or funnel management.

[320] *See* footnote 213

Observed traffic data

VR devices

Note the observed traffic for Pimax Pitool device is the same as the companion app and listed in the section below.

Table 30: Microsoft HoloLens 2 observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
client.wns.windows.com	NA	NA	NA	NA	NA	NA	NA	NA
inference.location.live.net	NA	NA	NA	NA	NA	NA	NA	NA
aka.ms	NA	NA	NA	NA	NA	NA	NA	NA
clientconfig.passport.net	NA	NA	NA	NA	NA	NA	NA	NA
substrate.office.com	NA	NA	NA	NA	NA	NA	NA	NA
login.live.com	live.com	No	No	No	No	No	No	No
displaycatalog.mp.microsoft.cc	microsoft.com	No	No	Yes	Yes	No	No	No
settings-win.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
sdx.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
licensing.mp.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
acctcdn.msauth.net	msauth.net	No	No	No	No	No	No	No
c.s-microsoft.com	s-microsoft.com	No	No	No	No	No	No	No
v10.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
nav.smartscreen.microsoft.con	microsoft.com	No	No	Yes	Yes	No	No	No
qcom-keyid-e7dc6c54fbc8a1a5f1ca4b957	azure.net	No	No	No	No	No	No	No
slscr.update.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
web.vortex.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
xsts.auth.xboxlive.com	xboxlive.com	No	No	No	No	No	No	No
account.live.com	live.com	No	No	No	No	No	No	No
fs.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
go.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
smartscreen-prod.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
storeedgefd.dsx.mp.microsoft.	microsoft.com	No	No	Yes	Yes	No	No	No
ajax.aspnetcdn.com	aspnetcdn.com	No	No	No	No	No	No	No
browser.events.data.microsoft	microsoft.com	No	No	Yes	Yes	No	No	No
continuum.dds.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
cs.dds.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
ekcert.spserv.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
fe3cr.delivery.mp.microsoft.co	microsoft.com	No	No	Yes	Yes	No	No	No
logincdn.msauth.net	msauth.net	No	No	No	No	No	No	No
privacy.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
title.auth.xboxlive.com	xboxlive.com	No	No	No	No	No	No	No
user.auth.xboxlive.com	xboxlive.com	No	No	No	No	No	No	No
v20.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
ztd.dds.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
device.auth.xboxlive.com	xboxlive.com	No	No	No	No	No	No	No

store-images.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
title.mgt.xboxlive.com	xboxlive.com	No	No	No	No	No	No	No
websockets.platform.bing.com	bing.com	Yes	Yes	Yes	Yes	No	No	No
www.msftconnecttest.com	NA	NA	NA	NA	NA	NA	NA	NA
img-prod-cms-rt-microsoft-com.akamaized.net	NA	NA	NA	NA	NA	NA	NA	NA
ctldl.windowsupdate.com	NA	NA	NA	NA	NA	NA	NA	NA
www.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
store-images.s-microsoft.com	s-microsoft.com	No	No	No	No	No	No	No
tpmsec.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
ocsp.digicert.com	digicert.com	No	No	No	No	No	No	No
	Total:	1	1	24	24	0	0	0

Table 31: HP Reverb G2 observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
img-prod-cms-rt-microsoft-com.akamaized.net	NA	NA	NA	NA	NA	NA	NA	NA
steamcommunity.com	NA	NA	NA	NA	NA	NA	NA	NA
fp-afd.azurefd.us	NA	NA	NA	NA	NA	NA	NA	NA
steamuserimages-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
api1.origin.com	NA	NA	NA	NA	NA	NA	NA	NA
fp-afd-nocache.azureedge.net	NA	NA	NA	NA	NA	NA	NA	NA
cxcs.microsoft.net	NA	NA	NA	NA	NA	NA	NA	NA
fp-afd.azureedge.net	NA	NA	NA	NA	NA	NA	NA	NA
fp-as-nocache.azureedge.net	NA	NA	NA	NA	NA	NA	NA	NA
steamstore-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
steamcdn-a.akamaihd.net	steamcdn-a.akamaihd.net	No	No	No	No	No	No	No
cdn.akamai.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
store.steampowered.com	steampowered.com	No	No	No	No	No	No	No
community.cloudflare.steamst	steamstatic.com	No	No	No	No	No	No	No
settings-win.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
moiawsorigin.clo.footprintdns.	footprintdns.com	No	No	No	No	No	No	No
login.live.com	live.com	No	No	No	No	No	No	No
self.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
cdn.cloudflare.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
arc.msn.com	msn.com	No	No	No	No	No	No	No
api.steampowered.com	steampowered.com	No	No	No	No	No	No	No
cm2-ord1.cm.steampowered.com	steampowered.com	No	No	No	No	No	No	No

cm6-lax1.cm.steampowered.com	steampowered.com	No	No	No	No	No	No	No
ow1.res.office365.com	office365.com	No	No	No	No	No	No	No
spo-ring.msedge.net	msedge.net	No	No	No	No	No	No	No
store.akamai.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
umwatson.events.data.microsc	microsoft.com	No	No	Yes	Yes	No	No	No
4bf57a62e33bf273f06eba818	footprintdns.com	No	No	No	No	No	No	No
a-ring-fallback.msedge.net	msedge.net	No	No	No	No	No	No	No
a-ring.msedge.net	msedge.net	No	No	No	No	No	No	No
b-ring.msedge.net	msedge.net	No	No	No	No	No	No	No
c-ring.msedge.net	msedge.net	No	No	No	No	No	No	No
checkappexec.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
eafd-dod-384ea1aa-6aab-4841-a754-35b60cef4ac8.azureedge.us	azureedge.us	No	No	No	No	No	No	No
fp-afd.azureedge.us	azureedge.us	No	No	No	No	No	No	No
fp.msedge.net	msedge.net	No	No	No	No	No	No	No
k-ring.msedge.net	msedge.net	No	No	No	No	No	No	No
l-ring.msedge.net	msedge.net	No	No	No	No	No	No	No
s-ring.msedge.net	msedge.net	No	No	No	No	No	No	No
t-ring.msedge.net	msedge.net	No	No	No	No	No	No	No
teams-ring.msedge.net	msedge.net	No	No	No	No	No	No	No
v10.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
www.bing.com	bing.com	Yes	Yes	Yes	Yes	No	No	No
ctldl.windowsupdate.com	NA	NA	NA	NA	NA	NA	NA	NA
r3.o.lencr.org	NA	NA	NA	NA	NA	NA	NA	NA
steamcommunity.com	NA	NA	NA	NA	NA	NA	NA	NA
x1.c.lencr.org	NA	NA	NA	NA	NA	NA	NA	NA
x2.c.lencr.org	NA	NA	NA	NA	NA	NA	NA	NA
go.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
api.steampowered.com	steampowered.com	No	No	No	No	No	No	No
ocsp.digicert.com	digicert.com	No	No	No	No	No	No	No
clientconfig.akamai.steamstati	steamstatic.com	No	No	No	No	No	No	No
dmd.metaservices.microsoft.c	microsoft.com	No	No	Yes	Yes	No	No	No
	Total:	1	1	8	8	0	0	0

Table 32: HTC Vive Cosmos Elite observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
vr-hwdl.vive.com	NA	NA	NA	NA	NA	NA	NA	NA
apu-chin2.htc.com	NA	NA	NA	NA	NA	NA	NA	NA
apu-msg2.htc.com	NA	NA	NA	NA	NA	NA	NA	NA
store.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
vrbi.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
contentstore.htcvive.com	NA	NA	NA	NA	NA	NA	NA	NA

account.htcvive.com	NA	NA	NA	NA	NA	NA	NA	NA
account-profile.htcvive.com	NA	NA	NA	NA	NA	NA	NA	NA
api1.origin.com	NA	NA	NA	NA	NA	NA	NA	NA
assets-global.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
steam-chat.com	NA	NA	NA	NA	NA	NA	NA	NA
vrbi.htcvive.com	NA	NA	NA	NA	NA	NA	NA	NA
www.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
v10.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
umwatson.events.data.microsc	microsoft.com	No	No	Yes	Yes	No	No	No
fe3cr.delivery.mp.microsoft.co	microsoft.com	No	No	Yes	Yes	No	No	No
fe2cr.update.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
api.steampowered.com	steampowered.com	No	No	No	No	No	No	No
058-suw-894.mktoresp.com	mktoresp.com	No	No	Yes	Yes	No	No	Yes
analytics.twitter.com	twitter.com	No	No	Yes	Yes	No	Yes	No
cdn.cloudflare.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
cm2-atl1.cm.steampowered.com	steampowered.com	No	No	No	No	No	No	No
cm5-lax1.cm.steampowered.com	steampowered.com	No	No	No	No	No	No	No
cs.dds.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
l.getsitecontrol.com	getsitecontrol.com	No	No	Yes	No	Yes	No	Yes
r2—sn-qxoedn7k.gvt1.com	gvt1.com	No	No	No	No	No	No	No
login.live.com	live.com	No	No	No	No	No	No	No
r5—sn-qxoedn7k.gvt1.com	gvt1.com	No	No	No	No	No	No	No
redirector.gvt1.com	gvt1.com	No	No	No	No	No	No	No
sdk-api-v1.singular.net	singular.net	No	No	No	No	No	No	No
static.ads-twitter.com	ads-twitter.com	Yes	No	Yes	Yes	No	No	Yes
widgets.getsitecontrol.com	getsitecontrol.com	No	No	Yes	No	Yes	No	Yes
t.co	t.co	No	No	Yes	Yes	Yes	Yes	No
insight.adsrvr.org	adsrvr.org	No	No	Yes	Yes	No	No	No
www.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
www.google-analytics.com	google-analytics.com	No	No	No	Yes	Yes	No	Yes
www.googletagmanager.com	googletagmanager.com	No	No	Yes	Yes	Yes	No	Yes
googleads.g.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
stats.g.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
dl.google.com	google.com	No	No	Yes	Yes	No	No	No
www.google.com	google.com	No	No	Yes	Yes	No	No	No
dl4.htc.com	NA	NA	NA	NA	NA	NA	NA	NA
go.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
clientconfig.akamai.steamstati	steamstatic.com	No	No	No	No	No	No	No
dmd.metaservices.microsoft.c	microsoft.com	No	No	Yes	Yes	No	No	No
	Total:	2	1	20	19	6	3	6

Table 33: PlayStation VR observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
ps5.np.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
qgve.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
vulcan.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
uef.np.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
fus01.ps5.update.playstation.r	NA	NA	NA	NA	NA	NA	NA	NA
control-center.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
ppr-crl.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
envelope2.np.dl.playstation.ne	NA	NA	NA	NA	NA	NA	NA	NA
home.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
monte-carlo.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
player-selection-dialog.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
gs-sec.ww.np.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
invitation-dialog.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
millenniumfalcon.rnps.dl.plays	NA	NA	NA	NA	NA	NA	NA	NA
sgst.prod.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
action-cards-host-app.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
agent-popupgui.rnps.dl.playstation.n	NA	NA	NA	NA	NA	NA	NA	NA
bgft.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
broadcast.rnps.dl.playstation.r	NA	NA	NA	NA	NA	NA	NA	NA
compilation-disc-hub.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
cosmiccube.rnps.dl.playstation	NA	NA	NA	NA	NA	NA	NA	NA
elysion.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
explore-hub.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
g2p-dialog.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
game-hub-preview-launcher.rnps.dl.playstation.ne	NA	NA	NA	NA	NA	NA	NA	NA
game-hub.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
gaming-lounge.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
igc-browse.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
legal-docs.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA

lfps-bc.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
library.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
millenniumfalcon-dialog.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
notification-overlay.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
onboard-download.rnps.dl.playstation.n	NA	NA	NA	NA	NA	NA	NA	NA
player-review.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
ppr-bgs.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
profile-dialog.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
profile.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
screen-share.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
search.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
service-hub-psnow.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
service-hub-psplus.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
system-message-client.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
titlestore-preview.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
trophy.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
universal-checkout.rnps.dl.playstation.ne	NA	NA	NA	NA	NA	NA	NA	NA
unsupported-title-hub.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
x-wing.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
psvrdd3.api.wwsga.me	NA	NA	NA	NA	NA	NA	NA	NA
psndocs.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
asm.np.community.playstation	NA	NA	NA	NA	NA	NA	NA	NA
alb001-pushcl.np.communication.play	NA	NA	NA	NA	NA	NA	NA	NA
ivt.np.community.playstation.n	NA	NA	NA	NA	NA	NA	NA	NA
psn-rsc.prod.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
static-resource.np.community.playst	NA	NA	NA	NA	NA	NA	NA	NA
id.sonyentertainmentnetwork.	NA	NA	NA	NA	NA	NA	NA	NA
occ-0-586-590.1.nflxso.net	NA	NA	NA	NA	NA	NA	NA	NA
trophy.ww.np.community.plays	NA	NA	NA	NA	NA	NA	NA	NA

xgen-title-map.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
35-167-30-174-pushcl.np.communication.plays	NA	NA	NA	NA	NA	NA	NA	NA
44-232-150-122-pushcl.np.communication.plays	NA	NA	NA	NA	NA	NA	NA	NA
44-234-157-111-pushcl.np.communication.plays	NA	NA	NA	NA	NA	NA	NA	NA
44-234-157-54-pushcl.np.communication.plays	NA	NA	NA	NA	NA	NA	NA	NA
activity.api.np.km.playstation.r	NA	NA	NA	NA	NA	NA	NA	NA
auth.api.np.ac.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
auth.api.sonyentertainmentne	NA	NA	NA	NA	NA	NA	NA	NA
commerce.api.np.km.playstatic	NA	NA	NA	NA	NA	NA	NA	NA
image.api.np.km.playstation.ne	NA	NA	NA	NA	NA	NA	NA	NA
psnobj.prod.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
sony-monte-carlo.prod.partner.netflix.net	NA	NA	NA	NA	NA	NA	NA	NA
us-prof.np.community.playstation	NA	NA	NA	NA	NA	NA	NA	NA
smetrics.aem.playstation.com	playstation.com	No	No	No	No	No	No	No
telemetry-console.api.playstation.com	playstation.com	No	No	No	No	No	No	No
image.api.playstation.com	playstation.com	No	No	No	No	No	No	No
store.playstation.com	playstation.com	No	No	No	No	No	No	No
urlconfig.api.playstation.com	playstation.com	No	No	No	No	No	No	No
primus.api.playstation.com	playstation.com	No	No	No	No	No	No	No
gmedia.playstation.com	playstation.com	No	No	No	No	No	No	No
static.playstation.com	playstation.com	No	No	No	No	No	No	No
www.playstation.com	playstation.com	No	No	No	No	No	No	No
collection.decibelinsight.net	decibelinsight.net	No	No	No	No	No	No	No
cdn.decibelinsight.net	decibelinsight.net	No	No	No	No	No	No	No
dmp.v.fwmrm.net	fwmrm.net	No	No	Yes	Yes	No	No	Yes
cm.everesttech.net	everesttech.net	No	No	Yes	No	No	No	Yes
lists.api.playstation.com	playstation.com	No	No	No	No	No	No	No
piyp.software.eu.playstation.cc	playstation.com	No	No	No	No	No	No	No
c.evidon.com	evidon.com	No	No	No	No	No	No	Yes
social.playstation.com	playstation.com	No	No	No	No	No	No	No
l.evidon.com	evidon.com	No	No	No	No	No	No	Yes
takedown.api.playstation.com	playstation.com	No	No	No	No	No	No	No
telemetry.api.playstation.com	playstation.com	No	No	No	No	No	No	No
web-toolbar.playstation.com	playstation.com	No	No	No	No	No	No	No
web.np.playstation.com	playstation.com	No	No	No	No	No	No	No
static-cdn.jtvnw.net	jtvnw.net	No	No	No	No	No	No	No
dpm.demdex.net	demdex.net	No	No	Yes	Yes	No	No	Yes

i.ytimg.com	ytimg.com	No	No	No	No	No	No	No
sne.demdex.net	demdex.net	No	No	Yes	Yes	No	No	Yes
sonynetworkentertain.tt.omtr	omtrdc.net	No	No	Yes	Yes	Yes	No	Yes
www.youtube.com	youtube.com	No	No	Yes	No	No	No	No
assets.adobedtm.com	adobedtm.com	No	No	Yes	No	Yes	No	Yes
gs2.ww.prod.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
static-resource.np.community.playst	NA	NA	NA	NA	NA	NA	NA	NA
gst.prod.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
fus01.ps5.update.playstation.n	NA	NA	NA	NA	NA	NA	NA	NA
ena.net.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
hus01.ps5.update.playstation.n	NA	NA	NA	NA	NA	NA	NA	NA
trophy01.np.community.playst	NA	NA	NA	NA	NA	NA	NA	NA
dus01.ps5.update.playstation.n	NA	NA	NA	NA	NA	NA	NA	NA
ic.18095300.09e87a.gs2.sony e.llnwd.net	llnwd.net	No	No	No	No	No	No	No
ic.18095300.05fa17.gs2.sony e.llnwd.net	llnwd.net	No	No	No	No	No	No	No
	Total:	0	0	7	4	2	0	8

Table 34: Meta Quest 2 observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
graph.oculus.com	NA	NA	NA	NA	NA	NA	NA	NA
cdn.felixandpaul.com	NA	NA	NA	NA	NA	NA	NA	NA
scontent.oculuscdn.com	NA	NA	NA	NA	NA	NA	NA	NA
securecdn.oculus.com	NA	NA	NA	NA	NA	NA	NA	NA
graph.facebook-hardware.com	NA	NA	NA	NA	NA	NA	NA	NA
www.felixandpaul.com	NA	NA	NA	NA	NA	NA	NA	NA
graph.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
mqtt-mini.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
rupload.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
www.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
scontent.fapa1-2.fna.fbcdn.net	fbcdn.net	Yes	No	No	No	No	Yes	No
www.google.com	google.com	No	No	Yes	Yes	No	No	No
portal.fb.com	fb.com	No	No	No	No	No	No	No
connectivitycheck.gstatic.com	gstatic.com	No	No	No	No	No	No	No
	Total:	5	4	5	5	4	5	0

Table 35: Valve Index observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
steam-chat.com	NA	NA	NA	NA	NA	NA	NA	NA

gameplay.intel.com	NA	NA	NA	NA	NA	NA	NA	NA
steamstore-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
steam-chat.com	NA	NA	NA	NA	NA	NA	NA	NA
steamcommunity.com	NA	NA	NA	NA	NA	NA	NA	NA
steamuserimages-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
steamstore-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
steamcommunity.com	NA	NA	NA	NA	NA	NA	NA	NA
steamuserimages-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
steam-chat.com	NA	NA	NA	NA	NA	NA	NA	NA
steamstore-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
steamcommunity.com	NA	NA	NA	NA	NA	NA	NA	NA
steamuserimages-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
steam-chat.com	NA	NA	NA	NA	NA	NA	NA	NA
steamstore-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
store.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
steamuserimages-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
steamcommunity.com	NA	NA	NA	NA	NA	NA	NA	NA
assets-global.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
apu-chin2.htc.com	NA	NA	NA	NA	NA	NA	NA	NA
account.htcvive.com	NA	NA	NA	NA	NA	NA	NA	NA
public-ubiservices.ubi.com	NA	NA	NA	NA	NA	NA	NA	NA
steamstore-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
vrbi.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
account-profile.htcvive.com	NA	NA	NA	NA	NA	NA	NA	NA
channel-service.upc.ubi.com	NA	NA	NA	NA	NA	NA	NA	NA
dmx.upc.ubisoft.com	NA	NA	NA	NA	NA	NA	NA	NA
gameplay.intel.com	NA	NA	NA	NA	NA	NA	NA	NA
steamcommunity-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
toggles.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
public-ws-ubiservices.ubi.com	NA	NA	NA	NA	NA	NA	NA	NA
ubistatic3-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
www.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
v10.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
fe3cr.delivery.mp.microsoft.co	microsoft.com	No	No	Yes	Yes	No	No	No
fe2cr.update.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
api.steampowered.com	steampowered.com	No	No	No	No	No	No	No
cdn.akamai.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
array510.prod.do.dsp.mp.micr	microsoft.com	No	No	Yes	Yes	No	No	No
checkappexec.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No

cm2-dfw1.cm.steampowered.com	steampowered.com	No	No	No	No	No	No	No
community.akamai.steamstatic	steamstatic.com	No	No	No	No	No	No	No
geo.prod.do.dsp.mp.microsoft.	microsoft.com	No	No	Yes	Yes	No	No	No
r1—sn-qxo7rn7l.gvt1.com	gvt1.com	No	No	No	No	No	No	No
redirector.gvt1.com	gvt1.com	No	No	No	No	No	No	No
settings-win.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
store.steampowered.com	steampowered.com	No	No	No	No	No	No	No
v10.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
community.akamai.steamstatic	steamstatic.com	No	No	No	No	No	No	No
steamcdn-a.akamaihd.net	steamcdn-a.akamaihd.net	No	No	No	No	No	No	No
cdn.akamai.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
api.steampowered.com	steampowered.com	No	No	No	No	No	No	No
fe3cr.delivery.mp.microsoft.co	microsoft.com	No	No	Yes	Yes	No	No	No
fe2cr.update.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
array510.prod.do.dsp.mp.micr	microsoft.com	No	No	Yes	Yes	No	No	No
store.steampowered.com	steampowered.com	No	No	No	No	No	No	No
checkappexec.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
cdp.cloud.unity3d.com	unity3d.com	No	No	No	No	No	No	No
cm2-dfw1.cm.steampowered.com	steampowered.com	No	No	No	No	No	No	No
config.uca.cloud.unity3d.com	unity3d.com	No	No	No	No	No	No	No
geo.prod.do.dsp.mp.microsoft.	microsoft.com	No	No	Yes	Yes	No	No	No
r1—sn-qxo7rn7l.gvt1.com	gvt1.com	No	No	No	No	No	No	No
redirector.gvt1.com	gvt1.com	No	No	No	No	No	No	No
store.akamai.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
steamcdn-a.akamaihd.net	steamcdn-a.akamaihd.net	No	No	No	No	No	No	No
cdn.akamai.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
store.steampowered.com	steampowered.com	No	No	No	No	No	No	No
community.akamai.steamstatic	steamstatic.com	No	No	No	No	No	No	No
api.steampowered.com	steampowered.com	No	No	No	No	No	No	No
arc.msn.com	msn.com	No	No	No	No	No	No	No
cdn.cloudflare.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
cdp.cloud.unity3d.com	unity3d.com	No	No	No	No	No	No	No
array510.prod.do.dsp.mp.micr	microsoft.com	No	No	Yes	Yes	No	No	No
cm2-dfw1.cm.steampowered.com	steampowered.com	No	No	No	No	No	No	No
checkappexec.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
config.uca.cloud.unity3d.com	unity3d.com	No	No	No	No	No	No	No
r1—sn-qxo7rn7l.gvt1.com	gvt1.com	No	No	No	No	No	No	No
geo.prod.do.dsp.mp.microsoft.	microsoft.com	No	No	Yes	Yes	No	No	No
redirector.gvt1.com	gvt1.com	No	No	No	No	No	No	No

ris.api.iris.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
settings-win.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
store.akamai.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
v10.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
wdcp.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
steamcdn-a.akamaihd.net	steamcdn-a.akamaihd.net	No	No	No	No	No	No	No
cdn.akamai.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
v10.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
store.steampowered.com	steampowered.com	No	No	No	No	No	No	No
community.akamai.steamstatic	steamstatic.com	No	No	No	No	No	No	No
api.steampowered.com	steampowered.com	No	No	No	No	No	No	No
cdn.cloudflare.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
fe2cr.update.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
fe3cr.delivery.mp.microsoft.co	microsoft.com	No	No	Yes	Yes	No	No	No
arc.msn.com	msn.com	No	No	No	No	No	No	No
cdp.cloud.unity3d.com	unity3d.com	No	No	No	No	No	No	No
array510.prod.do.dsp.mp.micr	microsoft.com	No	No	Yes	Yes	No	No	No
cm2-dfw1.cm.steampowered.com	steampowered.com	No	No	No	No	No	No	No
checkappexec.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
config.uca.cloud.unity3d.com	unity3d.com	No	No	No	No	No	No	No
geo.prod.do.dsp.mp.microsoft.	microsoft.com	No	No	Yes	Yes	No	No	No
r1—sn-qxo7rn7l.gvt1.com	gvt1.com	No	No	No	No	No	No	No
redirector.gvt1.com	gvt1.com	No	No	No	No	No	No	No
ris.api.iris.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
settings-win.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
steamcdn-a.akamaihd.net	steamcdn-a.akamaihd.net	No	No	No	No	No	No	No
store.akamai.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
v10.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
fe3cr.delivery.mp.microsoft.co	microsoft.com	No	No	Yes	Yes	No	No	No
cdn.akamai.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
store.steampowered.com	steampowered.com	No	No	No	No	No	No	No
fe2cr.update.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
community.akamai.steamstatic	steamstatic.com	No	No	No	No	No	No	No
cm6-iad1.cm.steampowered.com	steampowered.com	No	No	No	No	No	No	No
cm5-iad1.cm.steampowered.com	steampowered.com	No	No	No	No	No	No	No
cdn.cloudflare.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
api.steampowered.com	steampowered.com	No	No	No	No	No	No	No

cm2-dfw1.cm.steampowered.com	steampowered.com	No	No	No	No	No	No	No
cm3-iad1.cm.steampowered.com	steampowered.com	No	No	No	No	No	No	No
cm4-iad1.cm.steampowered.com	steampowered.com	No	No	No	No	No	No	No
store.akamai.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
umwatson.events.data.microsc	microsoft.com	No	No	Yes	Yes	No	No	No
array511.prod.do.dsp.mp.micr	microsoft.com	No	No	Yes	Yes	No	No	No
cm1-sea1.cm.steampowered.com	steampowered.com	No	No	No	No	No	No	No
settings-win.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
login.live.com	live.com	No	No	No	No	No	No	No
058-suw-894.mktoresp.com	mktoresp.com	No	No	Yes	Yes	No	No	Yes
arc.msn.com	msn.com	No	No	No	No	No	No	No
cm1-dfw1.cm.steampowered.com	steampowered.com	No	No	No	No	No	No	No
cm2-iad1.cm.steampowered.com	steampowered.com	No	No	No	No	No	No	No
array510.prod.do.dsp.mp.micr	microsoft.com	No	No	Yes	Yes	No	No	No
analytics.twitter.com	twitter.com	No	No	Yes	Yes	No	Yes	No
disc501.prod.do.dsp.mp.micros	microsoft.com	No	No	Yes	Yes	No	No	No
dash.getsitecontrol.com	getsitecontrol.com	No	No	Yes	No	Yes	No	Yes
l.getsitecontrol.com	getsitecontrol.com	No	No	Yes	No	Yes	No	Yes
lfghub-anonymous.xboxlive.com	xboxlive.com	No	No	No	No	No	No	No
polyfill.io	polyfill.io	No	No	No	No	No	No	No
ris.api.iris.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
static.ads-twitter.com	ads-twitter.com	Yes	No	Yes	Yes	No	No	Yes
t.co	t.co	No	No	Yes	Yes	Yes	Yes	No
wdcp.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
widgets.getsitecontrol.com	getsitecontrol.com	No	No	Yes	No	Yes	No	Yes
www.xboxab.com	xboxab.com	No	No	No	No	No	No	No
insight.adsrvr.org	adsrvr.org	No	No	Yes	Yes	No	No	No
www.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
steamcloud-us-west1.storage.googleapis.com	storage.googleapis.com	No	No	No	No	No	No	No
steamcloud-us-west1.storage.googleapis.com	storage.googleapis.com	No	No	No	No	No	No	No
steamcloud-us-west1.storage.googleapis.com	storage.googleapis.com	No	No	No	No	No	No	No
www.googleadservices.com	googleadservices.com	No	No	Yes	Yes	No	No	No
www.googletagmanager.com	googletagmanager.com	No	No	Yes	Yes	Yes	No	Yes
www.google-analytics.com	google-analytics.com	No	No	No	Yes	Yes	No	Yes
connect.facebook.net	facebook.net	Yes	Yes	Yes	Yes	Yes	Yes	No

stats.g.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
googleads.g.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
www.google.com	google.com	No	No	Yes	Yes	No	No	No
ctldl.windowsupdate.com	NA	NA	NA	NA	NA	NA	NA	NA
crl.identrust.com	NA	NA	NA	NA	NA	NA	NA	NA
x1.c.lencr.org	NA	NA	NA	NA	NA	NA	NA	NA
ctldl.windowsupdate.com	NA	NA	NA	NA	NA	NA	NA	NA
steamcommunity.com	NA	NA	NA	NA	NA	NA	NA	NA
crl.identrust.com	NA	NA	NA	NA	NA	NA	NA	NA
steamcommunity.com	NA	NA	NA	NA	NA	NA	NA	NA
ctldl.windowsupdate.com	NA	NA	NA	NA	NA	NA	NA	NA
crl.identrust.com	NA	NA	NA	NA	NA	NA	NA	NA
x1.c.lencr.org	NA	NA	NA	NA	NA	NA	NA	NA
steamcommunity.com	NA	NA	NA	NA	NA	NA	NA	NA
ctldl.windowsupdate.com	NA	NA	NA	NA	NA	NA	NA	NA
download.windowsupdate.com	NA	NA	NA	NA	NA	NA	NA	NA
crl.identrust.com	NA	NA	NA	NA	NA	NA	NA	NA
steamcommunity.com	NA	NA	NA	NA	NA	NA	NA	NA
ctldl.windowsupdate.com	NA	NA	NA	NA	NA	NA	NA	NA
store.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
crl.identrust.com	NA	NA	NA	NA	NA	NA	NA	NA
clientconfig.akamai.steamstati	steamstatic.com	No	No	No	No	No	No	No
dmd.metaservices.microsoft.c	microsoft.com	No	No	Yes	Yes	No	No	No
go.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
crash.steampowered.com	steampowered.com	No	No	No	No	No	No	No
steamcdn-a.akamaihd.net	steamcdn-a.akamaihd.net	No	No	No	No	No	No	No
api.steampowered.com	steampowered.com	No	No	No	No	No	No	No
clientconfig.akamai.steamstati	steamstatic.com	No	No	No	No	No	No	No
tile-service.weather.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
dmd.metaservices.microsoft.c	microsoft.com	No	No	Yes	Yes	No	No	No
go.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
crash.steampowered.com	steampowered.com	No	No	No	No	No	No	No
steamcdn-a.akamaihd.net	steamcdn-a.akamaihd.net	No	No	No	No	No	No	No
tile-service.weather.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
clientconfig.akamai.steamstati	steamstatic.com	No	No	No	No	No	No	No
api.steampowered.com	steampowered.com	No	No	No	No	No	No	No
crash.steampowered.com	steampowered.com	No	No	No	No	No	No	No
steamcdn-a.akamaihd.net	steamcdn-a.akamaihd.net	No	No	No	No	No	No	No
tile-service.weather.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No

clientconfig.akamai.steamstati	steamstatic.com	No	No	No	No	No	No	No
dmd.metaservices.microsoft.c	microsoft.com	No	No	Yes	Yes	No	No	No
go.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
api.steampowered.com	steampowered.com	No	No	No	No	No	No	No
crash.steampowered.com	steampowered.com	No	No	No	No	No	No	No
steamcdn-a.akamaihd.net	steamcdn-a.akamaihd.net	No	No	No	No	No	No	No
crash.steampowered.com	steampowered.com	No	No	No	No	No	No	No
clientconfig.akamai.steamstati	steamstatic.com	No	No	No	No	No	No	No
api.steampowered.com	steampowered.com	No	No	No	No	No	No	No
dmd.metaservices.microsoft.c	microsoft.com	No	No	Yes	Yes	No	No	No
go.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
tile-service.weather.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
	Total:	3	2	65	63	8	4	7

Companion apps

Table 36: Facebook observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
notifications-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
android.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
infinitedata-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
lookaside.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
b-api.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
graph.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
api.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
b-graph.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
edge-mqtt.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
mqtt-mini.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
www.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
connectivitycheck.gstatic.com	gstatic.com	No	No	No	No	No	No	No
android.apis.google.com	google.com	No	No	Yes	Yes	No	No	No
portal.fb.com	fb.com	No	No	No	No	No	No	No
	Total:	8	8	9	9	8	8	0

Table 37: Messenger observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
android.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
v.whatsapp.net	NA	NA	NA	NA	NA	NA	NA	NA
scontent-den4-1.xx.fbcdn.net	fbcdn.net	Yes	No	No	No	No	Yes	No
b-graph.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
lookaside.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
edge-mqtt.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
mqtt-mini.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
web.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
android.apis.google.com	google.com	No	No	Yes	Yes	No	No	No
portal.fb.com	fb.com	No	No	No	No	No	No	No
	Total:	6	5	6	6	5	6	0

Table 38: Microsoft App Store observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
windows.policies.live.net	NA	NA	NA	NA	NA	NA	NA	NA
storeedgefd.dsx.mp.microsoft.	microsoft.com	No	No	Yes	Yes	No	No	No
displaycatalog.mp.microsoft.cc	microsoft.com	No	No	Yes	Yes	No	No	No
login.live.com	live.com	No	No	No	No	No	No	No

v10.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
fe3cr.delivery.mp.microsoft.co	microsoft.com	No	No	Yes	Yes	No	No	No
smartscreen-prod.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
nav.smartscreen.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
title.auth.xboxlive.com	xboxlive.com	No	No	No	No	No	No	No
xsts.auth.xboxlive.com	xboxlive.com	No	No	No	No	No	No	No
settings-win.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
static.nvidiagrid.net	nvidiagrid.net	No	No	No	No	No	No	No
user.auth.xboxlive.com	xboxlive.com	No	No	No	No	No	No	No
device.auth.xboxlive.com	xboxlive.com	No	No	No	No	No	No	No
cp501.prod.do.dsp.mp.microsc	microsoft.com	No	No	Yes	Yes	No	No	No
go.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
jcmsfd.account.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
kv501.prod.do.dsp.mp.microsc	microsoft.com	No	No	Yes	Yes	No	No	No
graph.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
pti.store.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
purchase.mp.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
licensing.mp.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
store-images.s-microsoft.com	s-microsoft.com	No	No	No	No	No	No	No
www.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
geo.prod.do.dsp.mp.microsoft.	microsoft.com	No	No	Yes	Yes	No	No	No
www.bing.com	bing.com	Yes	Yes	Yes	Yes	No	No	No
tlu.dl.delivery.mp.microsoft.co	microsoft.com	No	No	Yes	Yes	No	No	No
ocsp.digicert.com	digicert.com	No	No	No	No	No	No	No
dl.delivery.mp.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
store-images.s-microsoft.com	s-microsoft.com	No	No	No	No	No	No	No
	Total:	1	1	20	20	0	0	0

Table 39: Mixed reality portal observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
canvas-cdn-prod.azureedge.net	NA	NA	NA	NA	NA	NA	NA	NA
account.asus.com	NA	NA	NA	NA	NA	NA	NA	NA
sparkcdnwus2.azureedge.net	NA	NA	NA	NA	NA	NA	NA	NA
login.live.com	live.com	No	No	No	No	No	No	No
v10.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
fe3cr.delivery.mp.microsoft.co	microsoft.com	No	No	Yes	Yes	No	No	No
purchase.mp.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
cp501.prod.do.dsp.mp.microsc	microsoft.com	No	No	Yes	Yes	No	No	No

settings-win.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
arc.msn.com	msn.com	No	No	No	No	No	No	No
xsts.auth.xboxlive.com	xboxlive.com	No	No	No	No	No	No	No
displaycatalog.mp.microsoft.cc	microsoft.com	No	No	Yes	Yes	No	No	No
c-ring.msedge.net	msedge.net	No	No	No	No	No	No	No
fp.msedge.net	msedge.net	No	No	No	No	No	No	No
geo.prod.do.dsp.mp.microsoft.	microsoft.com	No	No	Yes	Yes	No	No	No
kv501.prod.do.dsp.mp.microsc	microsoft.com	No	No	Yes	Yes	No	No	No
self.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
spo-ring.msedge.net	msedge.net	No	No	No	No	No	No	No
teams-ring.msedge.net	msedge.net	No	No	No	No	No	No	No
www.bing.com	bing.com	Yes	Yes	Yes	Yes	No	No	No
x1.c.lencr.org	NA	NA	NA	NA	NA	NA	NA	NA
tlu.dl.delivery.mp.microsoft.co	microsoft.com	No	No	Yes	Yes	No	No	No
dl.delivery.mp.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
ocsp.digicert.com	digicert.com	No	No	No	No	No	No	No
store-images.s-microsoft.com	s-microsoft.com	No	No	No	No	No	No	No
go.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
dmd.metaservices.microsoft.cc	microsoft.com	No	No	Yes	Yes	No	No	No
	Total:	1	1	14	14	0	0	0

Table 40: Oculus app observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
graph.oculus.com	NA	NA	NA	NA	NA	NA	NA	NA
scontent.oculuscdn.com	NA	NA	NA	NA	NA	NA	NA	NA
pubsub.plex.tv	NA	NA	NA	NA	NA	NA	NA	NA
play.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
plex.tv	NA	NA	NA	NA	NA	NA	NA	NA
android.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
playbooks-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
podcasts.provider.plex.tv	NA	NA	NA	NA	NA	NA	NA	NA
update.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
www.oculus.com	NA	NA	NA	NA	NA	NA	NA	NA
youtubei.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
api.us-east-1.aiv-delivery.net	NA	NA	NA	NA	NA	NA	NA	NA
app-measurement.com	NA	NA	NA	NA	NA	NA	NA	NA
auth.oculus.com	NA	NA	NA	NA	NA	NA	NA	NA
beacons.gcp.gvt2.com	NA	NA	NA	NA	NA	NA	NA	NA
beacons.gvt2.com	NA	NA	NA	NA	NA	NA	NA	NA
chromesyncpasswords-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA

deviceintegritytokens-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
epg.provider.plex.tv	NA	NA	NA	NA	NA	NA	NA	NA
infinitedata-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
metadata.provider.plex.tv	NA	NA	NA	NA	NA	NA	NA	NA
music.provider.plex.tv	NA	NA	NA	NA	NA	NA	NA	NA
passwordsleakcheck-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
people-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
safebrowsing.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
userlocation.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
vod.provider.plex.tv	NA	NA	NA	NA	NA	NA	NA	NA
vzwappprofile.vzw.com	NA	NA	NA	NA	NA	NA	NA	NA
webshows.provider.plex.tv	NA	NA	NA	NA	NA	NA	NA	NA
www.fbthirdpartypixel.com	NA	NA	NA	NA	NA	NA	NA	NA
xtrapath2.izatcloud.net	NA	NA	NA	NA	NA	NA	NA	NA
cx.atdmt.com	atdmt.com	No	No	Yes	Yes	No	No	No
mobile-collector.newrelic.com	newrelic.com	No	No	No	No	No	No	No
www.googleapis.com	www.googleapis.com	No	No	No	No	No	No	No
images-na.ssl-images-amazon.com	ssl-images-amazon.com	No	No	No	No	No	No	No
mads.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
staticcdn.duckduckgo.com	duckduckgo.com	No	No	No	No	No	No	No
r1—sn-q4flrnel.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
analytics.twitter.com	twitter.com	No	No	Yes	Yes	No	Yes	No
api.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
device-metrics-us-2.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
duckduckgo.com	duckduckgo.com	No	No	No	No	No	No	No
firebaseinstallations.googleapi	firebaseinstallations.google	No	No	No	No	No	No	No
msh.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
r6—sn-q4fl6nle.gvt1.com	gvt1.com	No	No	No	No	No	No	No
static.ads-twitter.com	ads-twitter.com	Yes	No	Yes	Yes	No	No	Yes
t.co	t.co	No	No	Yes	Yes	Yes	Yes	No
www.redditstatic.com	redditstatic.com	Yes	No	Yes	No	No	No	No
static.xx.fbcdn.net	fbcdn.net	Yes	No	No	No	No	Yes	No
graph.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
video.fapa1-2.fna.fbcdn.net	fbcdn.net	Yes	No	No	No	No	Yes	No
scontent.fapa1-1.fna.fbcdn.net	fbcdn.net	Yes	No	No	No	No	Yes	No
scontent.fapa1-2.fna.fbcdn.net	fbcdn.net	Yes	No	No	No	No	Yes	No
www.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No

m.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
scontent.xx.fbcdn.net	fbcdn.net	Yes	No	No	No	No	Yes	No
video.fapa1-1.fna.fbcdn.net	fbcdn.net	Yes	No	No	No	No	Yes	No
edge-mqtt.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
edge-chat.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
i.ytimg.com	ytimg.com	No	No	No	No	No	No	No
m.secure.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
s.amazon-adsystem.com	amazon-adsystem.com	No	No	Yes	Yes	No	No	No
www.googleadservices.com	googleadservices.com	No	No	Yes	Yes	No	No	No
connectivitycheck.gstatic.com	gstatic.com	No	No	No	No	No	No	No
www.gstatic.com	gstatic.com	No	No	No	No	No	No	No
tags.tiqcdn.com	tiqcdn.com	No	No	Yes	Yes	Yes	No	Yes
www.googletagmanager.com	googletagmanager.com	No	No	Yes	Yes	Yes	No	Yes
connect.facebook.net	facebook.net	Yes	Yes	Yes	Yes	Yes	Yes	No
googleads.g.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
10227187.fls.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
ad.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
accounts.google.com	google.com	No	No	Yes	Yes	No	No	No
www.google.com	google.com	No	No	Yes	Yes	No	No	No
adservice.google.com	google.com	No	No	Yes	Yes	No	No	No
mtalk.google.com	google.com	No	No	Yes	Yes	No	No	No
android.clients.google.com	google.com	No	No	Yes	Yes	No	No	No
wallet.google.com	google.com	No	No	Yes	Yes	No	No	No
clients4.google.com	google.com	No	No	Yes	Yes	No	No	No
safebrowsing.google.com	google.com	No	No	Yes	Yes	No	No	No
edgedl.me.gvt1.com	gvt1.com	No	No	No	No	No	No	No
connectivitycheck.gstatic.com	gstatic.com	No	No	No	No	No	No	No
	Total:	16	8	32	27	11	16	7

Table 41: Oculus Home observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
graph.oculus.com	NA	NA	NA	NA	NA	NA	NA	NA
securecdn.oculus.com	NA	NA	NA	NA	NA	NA	NA	NA
scontent.oculuscdn.com	NA	NA	NA	NA	NA	NA	NA	NA
api1.origin.com	NA	NA	NA	NA	NA	NA	NA	NA
ping-edge.smartscreen.microsoft.cc	microsoft.com	No	No	Yes	Yes	No	No	No
self.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
checkappexec.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
v10.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
graph.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No

scontent-den4-1.xx.fbcdn.net	fbcdn.net	Yes	No	No	No	No	Yes	No
	Total:	2	1	5	5	1	2	0

Table 42: PiTool Pimax observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
odoo.pimax.com	NA	NA	NA	NA	NA	NA	NA	NA
safebrowsing.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
v10.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
steamcdn-a.akamaihd.net	steamcdn-a.akamaihd.net	No	No	No	No	No	No	No
cdp.cloud.unity3d.com	unity3d.com	No	No	No	No	No	No	No
self.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
checkappexec.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
config.uca.cloud.unity3d.com	unity3d.com	No	No	No	No	No	No	No
cp501.prod.do.dsp.mp.microsc	microsoft.com	No	No	Yes	Yes	No	No	No
events.gfe.nvidia.com	nvidia.com	No	No	No	No	No	No	No
fe2cr.update.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
fe3cr.delivery.mp.microsoft.co	microsoft.com	No	No	Yes	Yes	No	No	No
cs.dds.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
geo.prod.do.dsp.mp.microsoft.	microsoft.com	No	No	Yes	Yes	No	No	No
kv501.prod.do.dsp.mp.microsc	microsoft.com	No	No	Yes	Yes	No	No	No
login.live.com	live.com	No	No	No	No	No	No	No
umwatson.events.data.microsc	microsoft.com	No	No	Yes	Yes	No	No	No
piserver.pimaxvr.com	NA	NA	NA	NA	NA	NA	NA	NA
download.windowsupdate.com	NA	NA	NA	NA	NA	NA	NA	NA
au.download.windowsupdate.c	NA	NA	NA	NA	NA	NA	NA	NA
clientconfig.akamai.steamstati	steamstatic.com	No	No	No	No	No	No	No
www.google-analytics.com	google-analytics.com	No	No	No	Yes	Yes	No	Yes
	Total:	0	0	10	11	1	0	1

Table 43: PlayStation observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
psn-rsc.prod.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
commerce.api.np.km.playstatic	NA	NA	NA	NA	NA	NA	NA	NA
eventcom.api.np.km.playstatio	NA	NA	NA	NA	NA	NA	NA	NA
id.sonyentertainmentnetwork.	NA	NA	NA	NA	NA	NA	NA	NA
static-resource.np.community.playst	NA	NA	NA	NA	NA	NA	NA	NA
youtubei.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
android.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
app-measurement.com	NA	NA	NA	NA	NA	NA	NA	NA

beacons.gvt2.com	NA	NA	NA	NA	NA	NA	NA	NA
content-autofill.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
infinitedata-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
people-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
play-fe.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
play.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
safebrowsing.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
theia.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
update.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
ca.account.sony.com	sony.com	No	No	No	No	No	No	No
device-api.urbanairship.com	urbanairship.com	No	No	No	No	No	No	No
my.account.sony.com	sony.com	No	No	No	No	No	No	No
redirector.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
image.api.playstation.com	playstation.com	No	No	No	No	No	No	No
telemetry.api.playstation.com	playstation.com	No	No	No	No	No	No	No
dms.api.playstation.com	playstation.com	No	No	No	No	No	No	No
m.np.playstation.com	playstation.com	No	No	No	No	No	No	No
id-lookup.api.playstation.com	playstation.com	No	No	No	No	No	No	No
sbahn-publish.api.playstation.com	playstation.com	No	No	No	No	No	No	No
smetrics.aem.playstation.com	playstation.com	No	No	No	No	No	No	No
accounts.api.playstation.com	playstation.com	No	No	No	No	No	No	No
ajax.googleapis.com	ajax.googleapis.com	No	No	No	No	No	No	No
blog.playstation.com	playstation.com	No	No	No	No	No	No	No
combine.urbanairship.com	urbanairship.com	No	No	No	No	No	No	No
client-api.arkoselabs.com	arkoselabs.com	No	No	No	No	No	No	No
firebaseinstallations.googleapi	firebaseinstallations.google	No	No	No	No	No	No	No
privacytemplate.api.playstatio	playstation.com	No	No	No	No	No	No	No
s.btstatic.com	btstatic.com	Yes	No	Yes	Yes	No	No	Yes
remote-data.urbanairship.com	urbanairship.com	No	No	No	No	No	No	No
sessions.bugsnag.com	bugsnag.com	No	No	No	No	No	No	No
s.thebrighttag.com	thebrighttag.com	No	No	Yes	Yes	No	No	Yes
sky-srlc.account.sony.com	sony.com	No	No	No	No	No	No	No
web.np.playstation.com	playstation.com	No	No	No	No	No	No	No
www.googleapis.com	www.googleapis.com	No	No	No	No	No	No	No
i.ytimg.com	ytimg.com	No	No	No	No	No	No	No
dpm.demdex.net	demdex.net	No	No	Yes	Yes	No	No	Yes
www.googleadservices.com	googleadservices.com	No	No	Yes	Yes	No	No	No
connectivitycheck.gstatic.com	gstatic.com	No	No	No	No	No	No	No
assets.adobedtm.com	adobedtm.com	No	No	Yes	No	Yes	No	Yes
android.apis.google.com	google.com	No	No	Yes	Yes	No	No	No

www.google.com	google.com	No	No	Yes	Yes	No	No	No
accounts.google.com	google.com	No	No	Yes	Yes	No	No	No
edgedl.me.gvt1.com	gvt1.com	No	No	No	No	No	No	No
	Total:	1	0	8	7	1	0	4

Table 44: Steam VR Desktop observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
steamcommunity.com	NA	NA	NA	NA	NA	NA	NA	NA
steamuserimages-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
store.steampowered.com	steampowered.com	No	No	No	No	No	No	No
steamcdn-a.akamaihd.net	steamcdn-a.akamaihd.net	No	No	No	No	No	No	No
cdn.cloudflare.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
api.steampowered.com	steampowered.com	No	No	No	No	No	No	No
community.cloudflare.steamst	steamstatic.com	No	No	No	No	No	No	No
checkappexec.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
static.nvidiagrid.net	nvidiagrid.net	No	No	No	No	No	No	No
store.akamai.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
steamcommunity.com	NA	NA	NA	NA	NA	NA	NA	NA
crash.steampowered.com	steampowered.com	No	No	No	No	No	No	No
test.steampowered.com	steampowered.com	No	No	No	No	No	No	No
	Total:	0	0	1	1	0	0	0

Table 45: Viveport observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
assets-global.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
store.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
steamcommunity.com	NA	NA	NA	NA	NA	NA	NA	NA
steamuserimages-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
www.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
account-profile.htcvive.com	NA	NA	NA	NA	NA	NA	NA	NA
vrbi.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
account.htcvive.com	NA	NA	NA	NA	NA	NA	NA	NA
activity.windows.com	NA	NA	NA	NA	NA	NA	NA	NA
client.wns.windows.com	NA	NA	NA	NA	NA	NA	NA	NA
steamcdn-a.akamaihd.net	steamcdn-a.akamaihd.net	No	No	No	No	No	No	No
licensing.mp.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
cdn.akamai.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
api.steampowered.com	steampowered.com	No	No	No	No	No	No	No
cdn.cloudflare.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No

store.steampowered.com	steampowered.com	No	No	No	No	No	No	No
login.live.com	live.com	No	No	No	No	No	No	No
settings-win.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
bl3301.storage.live.com	live.com	No	No	No	No	No	No	No
cm5-lax1.cm.steampowered.com	steampowered.com	No	No	No	No	No	No	No
cm6-lax1.cm.steampowered.com	steampowered.com	No	No	No	No	No	No	No
community.cloudflare.steamst	steamstatic.com	No	No	No	No	No	No	No
continuum.dds.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
edge.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
config.edge.skype.com	skype.com	No	No	No	No	No	No	No
msedge.api.cdp.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
self.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
store.akamai.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
umwatson.events.data.microsc	microsoft.com	No	No	Yes	Yes	No	No	No
v10.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
steamcommunity.com	NA	NA	NA	NA	NA	NA	NA	NA
ctldl.windowsupdate.com	NA	NA	NA	NA	NA	NA	NA	NA
store.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
api.steampowered.com	steampowered.com	No	No	No	No	No	No	No
clientconfig.akamai.steamstati	steamstatic.com	No	No	No	No	No	No	No
vr-hwdl.vive.com	NA	NA	NA	NA	NA	NA	NA	NA
account.htcvive.com	NA	NA	NA	NA	NA	NA	NA	NA
store.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
apu-chin2.htc.com	NA	NA	NA	NA	NA	NA	NA	NA
api1.origin.com	NA	NA	NA	NA	NA	NA	NA	NA
apu-download.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
apu-msg2.htc.com	NA	NA	NA	NA	NA	NA	NA	NA
px.owneriq.net	owneriq.net	No	Yes	Yes	Yes	Yes	No	No
v10.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
fe2cr.update.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
fe3cr.delivery.mp.microsoft.co	microsoft.com	No	No	Yes	Yes	No	No	No
survey.survicate.com	survicate.com	No	No	No	No	No	No	No
058-suw-894.mktoresp.com	mktoresp.com	No	No	Yes	Yes	No	No	Yes
ads.stickyadstv.com	stickyadstv.com	No	No	Yes	Yes	No	No	No
bh.contextweb.com	contextweb.com	No	Yes	Yes	Yes	Yes	No	No
checkappexec.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
d.turn.com	turn.com	No	No	Yes	Yes	No	No	No
cdn.mouseflow.com	mouseflow.com	Yes	No	Yes	No	No	No	Yes
evoke-windowsservices-tas.msedge.net	msedge.net	No	No	No	No	No	No	No
ib.adnxs.com	adnxs.com	No	No	Yes	Yes	No	No	No

px.surveywall-api.survata.com	survata.com	No	No	Yes	Yes	Yes	No	Yes
lm.serving-sys.com	serving-sys.com	No	No	Yes	Yes	No	No	No
secure.insightexpressai.com	insightexpressai.com	No	No	Yes	Yes	Yes	No	No
self.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
settings-win.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
secure.adnxs.com	adnxs.com	No	No	Yes	Yes	No	No	No
su.addthis.com	addthis.com	No	No	Yes	Yes	Yes	No	Yes
ce.lijit.com	lijit.com	Yes	No	Yes	Yes	Yes	No	Yes
insight.adsrvr.org	adsrvr.org	No	No	Yes	Yes	No	No	No
dpm.demdex.net	demdex.net	No	No	Yes	Yes	No	No	Yes
s.amazon-adsystem.com	amazon-adsystem.com	No	No	Yes	Yes	No	No	No
pixel.rubiconproject.com	rubiconproject.com	No	No	Yes	Yes	No	No	No
token.rubiconproject.com	rubiconproject.com	No	No	Yes	Yes	No	No	No
www.bing.com	bing.com	Yes	Yes	Yes	Yes	No	No	No
download.windowsupdate.com	NA	NA	NA	NA	NA	NA	NA	NA
ctldl.windowsupdate.com	NA	NA	NA	NA	NA	NA	NA	NA
store.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
x1.c.lencr.org	NA	NA	NA	NA	NA	NA	NA	NA
clientconfig.akamai.steamstati	steamstatic.com	No	No	No	No	No	No	No
ocsp.digicert.com	digicert.com	No	No	No	No	No	No	No
go.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
store.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
account.htcvive.com	NA	NA	NA	NA	NA	NA	NA	NA
vr-hwdl.vive.com	NA	NA	NA	NA	NA	NA	NA	NA
vrbi.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
assets-global.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
blob-ns.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
apu-chin2.htc.com	NA	NA	NA	NA	NA	NA	NA	NA
www.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
contentstore.htcvive.com	NA	NA	NA	NA	NA	NA	NA	NA
toggles.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
mozilla.cloudflare-dns.com	NA	NA	NA	NA	NA	NA	NA	NA
account-asset.htcvive.com	NA	NA	NA	NA	NA	NA	NA	NA
account-profile.htcvive.com	NA	NA	NA	NA	NA	NA	NA	NA
api1.origin.com	NA	NA	NA	NA	NA	NA	NA	NA
apu-msg2.htc.com	NA	NA	NA	NA	NA	NA	NA	NA
firefox.settings.services.mozill	NA	NA	NA	NA	NA	NA	NA	NA
egg.htcsense.com	NA	NA	NA	NA	NA	NA	NA	NA
push.services.mozilla.com	NA	NA	NA	NA	NA	NA	NA	NA
safebrowsing.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
steamstore-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA

steamcdn-a.akamaihd.net	steamcdn-a.akamaihd.net	No	No	No	No	No	No	No
self.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
settings-win.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
058-suw-894.mktoresp.com	mktoresp.com	No	No	Yes	Yes	No	No	Yes
px.owneriq.net	owneriq.net	No	Yes	Yes	Yes	Yes	No	No
survey.survicate.com	survicate.com	No	No	No	No	No	No	No
login.live.com	live.com	No	No	No	No	No	No	No
l.getsitecontrol.com	getsitecontrol.com	No	No	Yes	No	Yes	No	Yes
ib.adnxs.com	adnxs.com	No	No	Yes	Yes	No	No	No
surveys-static.survicate.com	survicate.com	No	No	No	No	No	No	No
usersync.samplicio.us	samplicio.us	Yes	No	Yes	No	Yes	No	Yes
a.audrte.com	audrte.com	No	No	No	No	No	No	No
aa.agkn.com	agkn.com	No	No	Yes	Yes	No	No	No
action.dstillery.com	dstillery.com	No	No	No	No	No	No	No
ads.samba.tv	samba.tv	No	No	No	No	No	No	No
ads.stickyadstv.com	stickyadstv.com	No	No	Yes	Yes	No	No	No
amazon.partners.tremorhub.cc	tremorhub.com	No	No	Yes	Yes	No	No	No
analytics.twitter.com	twitter.com	No	No	Yes	Yes	No	Yes	No
api-js.mixpanel.com	mixpanel.com	Yes	No	No	No	Yes	No	Yes
bh.contextweb.com	contextweb.com	No	Yes	Yes	Yes	Yes	No	No
c1.adform.net	adform.net	No	Yes	Yes	Yes	Yes	No	No
cdn4.mxpnl.com	mxpnl.com	Yes	No	No	No	Yes	No	Yes
bs.serving-sys.com	serving-sys.com	No	No	Yes	Yes	No	No	No
cdn.mouseflow.com	mouseflow.com	Yes	No	Yes	No	No	No	Yes
checkappexec.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
config.teams.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
d.agkn.com	agkn.com	No	No	Yes	Yes	No	No	No
d.turn.com	turn.com	No	No	Yes	Yes	No	No	No
displaycatalog.mp.microsoft.cc	microsoft.com	No	No	Yes	Yes	No	No	No
d1eoo1tco6rr5e.cloudfront.ne	d1eoo1tco6rr5e.cloudfron	No	No	No	No	No	No	No
events.getsitectrl.com	getsitectrl.com	No	No	No	No	No	No	No
idsync.rlcdn.com	rlcdn.com	No	Yes	Yes	Yes	No	No	Yes
lciapi.ninthdecimal.com	ninthdecimal.com	No	No	No	No	Yes	No	No
lm.serving-sys.com	serving-sys.com	No	No	Yes	Yes	No	No	No
loadus.exelator.com	exelator.com	Yes	No	Yes	Yes	Yes	No	No
mid.rkdms.com	rkdms.com	No	No	Yes	Yes	No	No	Yes
ml314.com	ml314.com	Yes	No	Yes	Yes	Yes	No	No
munchkin.marketo.net	marketo.net	No	No	Yes	Yes	No	No	Yes
mwzeom.zeotap.com	zeotap.com	No	No	No	No	No	No	No
odr.mookie1.com	mookie1.com	Yes	No	Yes	Yes	Yes	No	Yes
match.sync.ad.cpe.dotomi.com	dotomi.com	No	No	Yes	Yes	No	No	No
pi.ispot.tv	ispot.tv	No	No	No	Yes	Yes	No	No

px.surveywall-api.survata.com	survata.com	No	No	Yes	Yes	Yes	No	Yes
pixel.advertising.com	advertising.com	No	No	Yes	Yes	No	No	No
s2.getsitecontrol.com	getsitecontrol.com	No	No	Yes	No	Yes	No	Yes
match.sharethrough.com	sharethrough.com	No	No	Yes	Yes	No	No	No
sdk-api-v1.singular.net	singular.net	No	No	No	No	No	No	No
sb.scorecardresearch.com	scorecardresearch.com	No	No	No	No	Yes	No	No
secure-gl.imrworldwide.com	imrworldwide.com	Yes	No	Yes	Yes	Yes	No	Yes
secure.adnxs.com	adnxs.com	No	No	Yes	Yes	No	No	No
static.ads-twitter.com	ads-twitter.com	Yes	No	Yes	Yes	No	No	Yes
store.steampowered.com	steampowered.com	No	No	No	No	No	No	No
stags.bluekai.com	bluekai.com	No	No	Yes	Yes	Yes	No	No
sync.search.spotxchange.com	spotxchange.com	No	No	Yes	Yes	No	No	No
www.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
su.addthis.com	addthis.com	No	No	Yes	Yes	Yes	No	Yes
insight.adsrvr.org	adsrvr.org	No	No	Yes	Yes	No	No	No
beacon.krxd.net	krxd.net	No	No	Yes	Yes	Yes	No	No
ce.lijit.com	lijit.com	Yes	No	Yes	Yes	Yes	No	Yes
dsum.casalemedia.com	casalemedia.com	No	No	Yes	Yes	No	No	No
dpm.demdex.net	demdex.net	No	No	Yes	Yes	No	No	Yes
dsum-sec.casalemedia.com	casalemedia.com	No	No	Yes	Yes	No	No	No
js.adsrvr.org	adsrvr.org	No	No	Yes	Yes	No	No	No
ssum-sec.casalemedia.com	casalemedia.com	No	No	Yes	Yes	No	No	No
sync.sharethis.com	sharethis.com	No	No	Yes	Yes	No	No	Yes
sync.crwdcntrl.net	crwdcntrl.net	No	No	Yes	Yes	Yes	No	No
s.amazon-adsystem.com	amazon-adsystem.com	No	No	Yes	Yes	No	No	No
pixel.rubiconproject.com	rubiconproject.com	No	No	Yes	Yes	No	No	No
cms.analytics.yahoo.com	yahoo.com	No	No	Yes	Yes	Yes	No	No
image2.pubmatic.com	pubmatic.com	No	Yes	Yes	Yes	Yes	No	Yes
image6.pubmatic.com	pubmatic.com	No	Yes	Yes	Yes	Yes	No	Yes
simage2.pubmatic.com	pubmatic.com	No	Yes	Yes	Yes	Yes	No	Yes
connect.facebook.net	facebook.net	Yes	Yes	Yes	Yes	Yes	Yes	No
googleads.g.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
bid.g.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
stats.g.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
www.google.com	google.com	No	No	Yes	Yes	No	No	No
cm.g.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
adservice.google.com	google.com	No	No	Yes	Yes	No	No	No
6698523.fls.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
apu-download.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
ctldl.windowsupdate.com	NA	NA	NA	NA	NA	NA	NA	NA
store.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
detectportal.firefox.com	NA	NA	NA	NA	NA	NA	NA	NA
ocsp.digicert.com	digicert.com	No	No	No	No	No	No	No

clientconfig.akamai.steamstati	steamstatic.com	No	No	No	No	No	No	No
vr-hwdl.vive.com	NA	NA	NA	NA	NA	NA	NA	NA
account.htcvive.com	NA	NA	NA	NA	NA	NA	NA	NA
apu-chin2.htc.com	NA	NA	NA	NA	NA	NA	NA	NA
store.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
vrbi.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
contentstore.htcvive.com	NA	NA	NA	NA	NA	NA	NA	NA
mozilla.cloudflare-dns.com	NA	NA	NA	NA	NA	NA	NA	NA
account-asset.htcvive.com	NA	NA	NA	NA	NA	NA	NA	NA
api1.origin.com	NA	NA	NA	NA	NA	NA	NA	NA
apu-msg2.htc.com	NA	NA	NA	NA	NA	NA	NA	NA
firefox.settings.services.mozill	NA	NA	NA	NA	NA	NA	NA	NA
toggles.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
www.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
push.services.mozilla.com	NA	NA	NA	NA	NA	NA	NA	NA
safebrowsing.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
steamstore-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
vrbi.htcvive.com	NA	NA	NA	NA	NA	NA	NA	NA
px.owneriq.net	owneriq.net	No	Yes	Yes	Yes	Yes	No	No
self.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
058-suw-894.mktoresp.com	mktoresp.com	No	No	Yes	Yes	No	No	Yes
v10.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
surveys-static.survicate.com	survicate.com	No	No	No	No	No	No	No
steamcdn-a.akamaihd.net	steamcdn-a.akamaihd.net	No	No	No	No	No	No	No
survey.survicate.com	survicate.com	No	No	No	No	No	No	No
ads.samba.tv	samba.tv	No	No	No	No	No	No	No
ads.stickyadstv.com	stickyadstv.com	No	No	Yes	Yes	No	No	No
amazon.partners.tremorhub.c	tremorhub.com	No	No	Yes	Yes	No	No	No
c1.adform.net	adform.net	No	Yes	Yes	Yes	Yes	No	No
bh.contextweb.com	contextweb.com	No	Yes	Yes	Yes	Yes	No	No
cdn.mouseflow.com	mouseflow.com	Yes	No	Yes	No	No	No	Yes
checkappexec.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
bs.serving-sys.com	serving-sys.com	No	No	Yes	Yes	No	No	No
d.turn.com	turn.com	No	No	Yes	Yes	No	No	No
lciapi.ninthdecimal.com	ninthdecimal.com	No	No	No	No	Yes	No	No
loadus.exelator.com	exelator.com	Yes	No	Yes	Yes	Yes	No	No
lm.serving-sys.com	serving-sys.com	No	No	Yes	Yes	No	No	No
ib.adnxs.com	adnxs.com	No	No	Yes	Yes	No	No	No
pixel.advertising.com	advertising.com	No	No	Yes	Yes	No	No	No
px.surveywall-api.survata.com	survata.com	No	No	Yes	Yes	Yes	No	Yes
match.sharethrough.com	sharethrough.com	No	No	Yes	Yes	No	No	No

settings-win.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
secure.adnxs.com	adnxs.com	No	No	Yes	Yes	No	No	No
sync.search.spotxchange.com	spotxchange.com	No	No	Yes	Yes	No	No	No
su.addthis.com	addthis.com	No	No	Yes	Yes	Yes	No	Yes
t.myvisualiq.net	myvisualiq.net	No	No	Yes	Yes	Yes	No	No
usersync.samplicio.us	samplicio.us	Yes	No	Yes	No	Yes	No	Yes
x.bidswitch.net	bidswitch.net	No	Yes	Yes	Yes	No	No	No
ce.lijit.com	lijit.com	Yes	No	Yes	Yes	Yes	No	Yes
beacon.krxd.net	krxd.net	No	No	Yes	Yes	Yes	No	No
dpm.demdex.net	demdex.net	No	No	Yes	Yes	No	No	Yes
insight.adsrvr.org	adsrvr.org	No	No	Yes	Yes	No	No	No
sync.sharethis.com	sharethis.com	No	No	Yes	Yes	No	No	Yes
ssum-sec.casalemedia.com	casalemedia.com	No	No	Yes	Yes	No	No	No
usermatch.krxd.net	krxd.net	No	No	Yes	Yes	Yes	No	No
sync.crwdcntrl.net	crwdcntrl.net	No	No	Yes	Yes	Yes	No	No
www.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
s.amazon-adsystem.com	amazon-adsystem.com	No	No	Yes	Yes	No	No	No
pixel.rubiconproject.com	rubiconproject.com	No	No	Yes	Yes	No	No	No
token.rubiconproject.com	rubiconproject.com	No	No	Yes	Yes	No	No	No
cms.analytics.yahoo.com	yahoo.com	No	No	Yes	Yes	Yes	No	No
ups.analytics.yahoo.com	yahoo.com	No	No	Yes	Yes	Yes	No	No
sync.taboola.com	taboola.com	No	No	Yes	Yes	Yes	No	Yes
connect.facebook.net	facebook.net	Yes	Yes	Yes	Yes	Yes	Yes	No
www.google.com	google.com	No	No	Yes	Yes	No	No	No
apu-download.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
ctldl.windowsupdate.com	NA	NA	NA	NA	NA	NA	NA	NA
detectportal.firefox.com	NA	NA	NA	NA	NA	NA	NA	NA
store.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
ocsp.digicert.com	digicert.com	No	No	No	No	No	No	No
clientconfig.akamai.steamstati	steamstatic.com	No	No	No	No	No	No	No
	Total:	21	18	139	133	51	5	36

Third-Party Apps

Table 46: Beat Saber observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
ps5.np.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
qgve.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
uef.np.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
asm.np.community.playstation	NA	NA	NA	NA	NA	NA	NA	NA
gs-sec.ww.np.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
trophy.ww.np.community.plays	NA	NA	NA	NA	NA	NA	NA	NA
ivt.np.community.playstation.n	NA	NA	NA	NA	NA	NA	NA	NA
action-cards-host-app.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
activity.api.np.km.playstation.r	NA	NA	NA	NA	NA	NA	NA	NA
agent-popupgui.rnps.dl.playstation.n	NA	NA	NA	NA	NA	NA	NA	NA
bgft.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
broadcast.rnps.dl.playstation.r	NA	NA	NA	NA	NA	NA	NA	NA
codex.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
compilation-disc-hub.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
control-center.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
cosmiccube.rnps.dl.playstation	NA	NA	NA	NA	NA	NA	NA	NA
elysion.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
explore-hub.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
feature-discovery-assets-amd.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
g2p-dialog.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
game-hub-preview-launcher.rnps.dl.playstation.ne	NA	NA	NA	NA	NA	NA	NA	NA
game-hub.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
gaming-lounge.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
getprof.us.np.community.plays	NA	NA	NA	NA	NA	NA	NA	NA
graph.oculus.com	NA	NA	NA	NA	NA	NA	NA	NA
home.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
igc-browse.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
invitation-dialog.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
legal-docs.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA

lfps-bc.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
library.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
loyalty-hub.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
millenniumfalcon-dialog.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
millenniumfalcon.rnps.dl.plays	NA		NA	NA	NA	NA	NA	NA	NA
monte-carlo.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
notification-overlay.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
onboard-download.rnps.dl.playstation.n	NA		NA	NA	NA	NA	NA	NA	NA
player-review.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
player-selection-dialog.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
ppr-bgs.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
ppr-crl.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
profile-dialog.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
profile.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
ps5-multi-bundle-ota.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
rnps-peripherals-onboarding.rnps.dl.playstation	NA		NA	NA	NA	NA	NA	NA	NA
screen-share.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
search.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
service-hub-psnow.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
service-hub-psplus.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
settings.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
system-message-client.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
titlestore-preview.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
trophy.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
uam-fs.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA
universal-checkout.rnps.dl.playstation.ne	NA		NA	NA	NA	NA	NA	NA	NA
unsupported-title-hub.rnps.dl.playstation.net	NA		NA	NA	NA	NA	NA	NA	NA

ut-service.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
wishlist.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
x-wing.rnps.dl.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
fus01.ps5.update.playstation.r	NA	NA	NA	NA	NA	NA	NA	NA
ranking-rec-l01.u0.np.community.playstati	NA	NA	NA	NA	NA	NA	NA	NA
uds-edge.np.community.playstatior	NA	NA	NA	NA	NA	NA	NA	NA
feature.api.playstation.com	playstation.com	No	No	No	No	No	No	No
takedown.api.playstation.com	playstation.com	No	No	No	No	No	No	No
i.scdn.co	scdn.co	No	No	No	No	No	No	No
telemetry-console.api.playstation.com	playstation.com	No	No	No	No	No	No	No
smetrics.aem.playstation.com	playstation.com	No	No	No	No	No	No	No
image.api.playstation.com	playstation.com	No	No	No	No	No	No	No
ranking-view-l01.u0.np.community.playstati	NA	NA	NA	NA	NA	NA	NA	NA
trophy01.np.community.playst	NA	NA	NA	NA	NA	NA	NA	NA
static-resource.np.community.playst	NA	NA	NA	NA	NA	NA	NA	NA
ena.net.playstation.net	NA	NA	NA	NA	NA	NA	NA	NA
	Total:	0	0	0	0	0	0	0

Table 47: Engage observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
store.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
app.engagevr.io	NA	NA	NA	NA	NA	NA	NA	NA
unity-cdn.engagevr.io	NA	NA	NA	NA	NA	NA	NA	NA
apu-chin2.htc.com	NA	NA	NA	NA	NA	NA	NA	NA
blob-ns.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
assets-global.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
steamcommunity.com	NA	NA	NA	NA	NA	NA	NA	NA
contentstore.htcvive.com	NA	NA	NA	NA	NA	NA	NA	NA
steamuserimages-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
account-profile.htcvive.com	NA	NA	NA	NA	NA	NA	NA	NA
account.htcvive.com	NA	NA	NA	NA	NA	NA	NA	NA
api1.origin.com	NA	NA	NA	NA	NA	NA	NA	NA
vrbi.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
toggles.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
web-assets.engagevr.io	NA	NA	NA	NA	NA	NA	NA	NA
ivre-web-assets.s3.eu-west-1.amazonaws.com	eu-west-1.amazonaws.com	No	No	No	No	No	No	No

steamcdn-a.akamaihd.net	steamcdn-a.akamaihd.net	No	No	No	No	No	No	No
cdn.cloudflare.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
self.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
store.steampowered.com	steampowered.com	No	No	No	No	No	No	No
login.live.com	live.com	No	No	No	No	No	No	No
api.steampowered.com	steampowered.com	No	No	No	No	No	No	No
static.nvidiagrid.net	nvidiagrid.net	No	No	No	No	No	No	No
api.msn.com	msn.com	No	No	No	No	No	No	No
cm6-lax1.cm.steampowered.com	steampowered.com	No	No	No	No	No	No	No
community.cloudflare.steamst	steamstatic.com	No	No	No	No	No	No	No
settings-win.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
store.akamai.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
umwatson.events.data.microsc	microsoft.com	No	No	Yes	Yes	No	No	No
v10.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
www.bing.com	bing.com	Yes	Yes	Yes	Yes	No	No	No
www.gstatic.com	gstatic.com	No	No	No	No	No	No	No
fonts.gstatic.com	gstatic.com	No	No	No	No	No	No	No
www.google.com	google.com	No	No	Yes	Yes	No	No	No
play.google.com	google.com	No	No	Yes	Yes	No	No	No
adservice.google.com	google.com	No	No	Yes	Yes	No	No	No
ogs.google.com	google.com	No	No	Yes	Yes	No	No	No
apis.google.com	google.com	No	No	Yes	Yes	No	No	No
ctldl.windowsupdate.com	NA	NA	NA	NA	NA	NA	NA	NA
store.viveport.com	NA	NA	NA	NA	NA	NA	NA	NA
steamcommunity.com	NA	NA	NA	NA	NA	NA	NA	NA
x1.c.lencr.org	NA	NA	NA	NA	NA	NA	NA	NA
clientconfig.akamai.steamstati	steamstatic.com	No	No	No	No	No	No	No
go.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
dmd.metaservices.microsoft.c	microsoft.com	No	No	Yes	Yes	No	No	No
api.steampowered.com	steampowered.com	No	No	No	No	No	No	No
test.steampowered.com	steampowered.com	No	No	No	No	No	No	No
	Total:	1	1	12	12	0	0	0

Table 48: Tiltbrush observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
graph.oculus.com	NA	NA	NA	NA	NA	NA	NA	NA
scontent.oculuscdn.com	NA	NA	NA	NA	NA	NA	NA	NA
graph.facebook-hardware.com	NA	NA	NA	NA	NA	NA	NA	NA
safebrowsing.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
vrassets-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA

graph.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
static.xx.fbcdn.net	fbcdn.net	Yes	No	No	No	No	Yes	No
mqtt-mini.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
scontent-den4-1.xx.fbcdn.net	fbcdn.net	Yes	No	No	No	No	Yes	No
ssl.gstatic.com	gstatic.com	No	No	No	No	No	No	No
fonts.gstatic.com	gstatic.com	No	No	No	No	No	No	No
www.google-analytics.com	google-analytics.com	No	No	No	Yes	Yes	No	Yes
accounts.google.com	google.com	No	No	Yes	Yes	No	No	No
www.google.com	google.com	No	No	Yes	Yes	No	No	No
play.google.com	google.com	No	No	Yes	Yes	No	No	No
connectivitycheck.gstatic.com	gstatic.com	No	No	No	No	No	No	No
	Total:	4	2	5	6	3	4	1

Table 49: VRChat observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
api.vrchat.cloud	NA	NA	NA	NA	NA	NA	NA	NA
assets.vrchat.com	NA	NA	NA	NA	NA	NA	NA	NA
steamuserimages-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
d348imysud55la.cloudfront.ne	NA	NA	NA	NA	NA	NA	NA	NA
steamcommunity.com	NA	NA	NA	NA	NA	NA	NA	NA
api1.origin.com	NA	NA	NA	NA	NA	NA	NA	NA
files.vrchat.cloud	NA	NA	NA	NA	NA	NA	NA	NA
fp-afd-nocache-ccp.azureedge.net	NA	NA	NA	NA	NA	NA	NA	NA
fp-afd-nocache.azureedge.net	NA	NA	NA	NA	NA	NA	NA	NA
hello.vrchat.com	NA	NA	NA	NA	NA	NA	NA	NA
pipeline.vrchat.cloud	NA	NA	NA	NA	NA	NA	NA	NA
steamcommunity-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
steamusercontent-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
steamcdn-a.akamaihd.net	steamcdn-a.akamaihd.net	No	No	No	No	No	No	No
login.live.com	live.com	No	No	No	No	No	No	No
store.steampowered.com	steampowered.com	No	No	No	No	No	No	No
cdn.cloudflare.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
api2.amplitude.com	amplitude.com	No	No	No	No	No	No	No
api.steampowered.com	steampowered.com	No	No	No	No	No	No	No
community.cloudflare.steamst	steamstatic.com	No	No	No	No	No	No	No
cdp.cloud.unity3d.com	unity3d.com	No	No	No	No	No	No	No
config.uca.cloud.unity3d.com	unity3d.com	No	No	No	No	No	No	No
cdn.akamai.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No

static.nvidiagrid.net	nvidiagrid.net	No	No	No	No	No	No	No
title.auth.xboxlive.com	xboxlive.com	No	No	No	No	No	No	No
cm5-lax1.cm.steampowered.com	steampowered.com	No	No	No	No	No	No	No
device.auth.xboxlive.com	xboxlive.com	No	No	No	No	No	No	No
events.gfe.nvidia.com	nvidia.com	No	No	No	No	No	No	No
self.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
settings-win.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
store.akamai.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
umwatson.events.data.microsc	microsoft.com	No	No	Yes	Yes	No	No	No
user.auth.xboxlive.com	xboxlive.com	No	No	No	No	No	No	No
xsts.auth.xboxlive.com	xboxlive.com	No	No	No	No	No	No	No
checkappexec.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
fp.msedge.net	msedge.net	No	No	No	No	No	No	No
lfghub-anonymous.xboxlive.com	xboxlive.com	No	No	No	No	No	No	No
s-ring.msedge.net	msedge.net	No	No	No	No	No	No	No
title.mgt.xboxlive.com	xboxlive.com	No	No	No	No	No	No	No
v10.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
static1.squarespace.com	squarespace.com	No	No	No	No	No	No	No
www.xboxab.com	xboxab.com	No	No	No	No	No	No	No
www.bing.com	bing.com	Yes	Yes	Yes	Yes	No	No	No
steamcommunity.com	NA	NA	NA	NA	NA	NA	NA	NA
piserver.pimaxvr.com	NA	NA	NA	NA	NA	NA	NA	NA
clientconfig.akamai.steamstati	steamstatic.com	No	No	No	No	No	No	No
test.steampowered.com	steampowered.com	No	No	No	No	No	No	No
crash.steampowered.com	steampowered.com	No	No	No	No	No	No	No
api.steampowered.com	steampowered.com	No	No	No	No	No	No	No
www.google-analytics.com	google-analytics.com	No	No	No	Yes	Yes	No	Yes
	Total:	1	1	6	7	1	0	1

Table 50: Windows Mixed Reality observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
steamcommunity.com	NA	NA	NA	NA	NA	NA	NA	NA
steamuserimages-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
steamstore-a.akamaihd.net	NA	NA	NA	NA	NA	NA	NA	NA
steamcdn-a.akamaihd.net	steamcdn-a.akamaihd.net	No	No	No	No	No	No	No
store.steampowered.com	steampowered.com	No	No	No	No	No	No	No
cdn.cloudflare.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
cdn.akamai.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
community.cloudflare.steamst	steamstatic.com	No	No	No	No	No	No	No

api.steampowered.com	steampowered.com	No	No	No	No	No	No	No
settings-win.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
store.akamai.steamstatic.com	steamstatic.com	No	No	No	No	No	No	No
static.nvidiagrid.net	nvidiagrid.net	No	No	No	No	No	No	No
steamcommunity.com	NA	NA	NA	NA	NA	NA	NA	NA
api.steampowered.com	steampowered.com	No	No	No	No	No	No	No
test.steampowered.com	steampowered.com	No	No	No	No	No	No	No
	Total:	0	0	1	1	0	0	0

Table 51: Youtube VR observed traffic

Source	Match Domain	AP	AF	AMT	AD	AM	SN	TPAM
api1.origin.com	NA	NA	NA	NA	NA	NA	NA	NA
safebrowsing.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
config.edge.skype.com	skype.com	No	No	No	No	No	No	No
self.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
v10.events.data.microsoft.com	microsoft.com	No	No	Yes	Yes	No	No	No
jnn-pa.googleapis.com	jnn-pa.googleapis.com	No	No	No	No	No	No	No
yt3.ggpht.com	ggpht.com	No	No	No	No	No	No	No
fonts.googleapis.com	fonts.googleapis.com	No	No	No	No	No	No	No
www.youtube.com	youtube.com	No	No	Yes	No	No	No	No
youtube.com	youtube.com	No	No	Yes	No	No	No	No
fonts.gstatic.com	gstatic.com	No	No	No	No	No	No	No
pagead2.googlesyndication.com	googlesyndication.com	No	No	Yes	Yes	No	No	No
tpc.googlesyndication.com	googlesyndication.com	No	No	Yes	Yes	No	No	No
googleads.g.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
accounts.google.com	google.com	No	No	Yes	Yes	No	No	No
static.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
play.google.com	google.com	No	No	Yes	Yes	No	No	No
www.google.com	google.com	No	No	Yes	Yes	No	No	No
ocsp.pki.goog	NA	NA	NA	NA	NA	NA	NA	NA
clientconfig.akamai.steamstati	steamstatic.com	No	No	No	No	No	No	No
	Total:	0	0	11	9	0	0	0

About Common Sense

Common Sense is the nation's leading nonprofit organization dedicated to improving the lives of all kids and families by providing the trustworthy information, education, and independent voice they need to thrive in the 21st century. Our independent research is designed to provide parents, educators, health organizations, and policymakers with reliable, independent data on children's use of media and technology and the impact it has on their physical, emotional, social, and intellectual development. For more information, visit privacy.commonsense.org

commonsense.org