Research shows VR poses privacy risks for kids—parents aren't as worried as they should be

May 6 2024, by Matt Shipman

Credit: Unsplash/CC0 Public Domain

New research finds that, while an increasing number of minors are using virtual reality (VR) apps, not many parents recognize the extent of the

security and privacy risks that are specific to VR technologies. The study also found that few parents are taking active steps to address those security and privacy issues, such as using parental controls built into the apps.

"In recent years we have seen an increase in the number of minors using VR apps that have social interaction elements, which increases security and privacy risks—such as unintended self-disclosures of sensitive personal information and surveillance of a user's biometric data," says Abhinaya S B, co-author of a paper on the work and a Ph.D. student at NC State.

"We wanted to see how much parents know about security and privacy risks associated with these VR apps, and what they are currently doing to address those risks," Abhinaya says. "These findings will help us identify areas where parents, technology designers, and policymakers could do more to enhance children's security and privacy."

For the study, researchers conducted in-depth interviews with 20 parents who have children under the age of 18 at home who use VR apps. The interviews were designed to capture what sort of risks parents perceived regarding VR apps, what strategies the parents used to protect their children's security and privacy in regard to VR apps, and which VR stakeholders the parents felt were responsible for protecting children who use the apps.

"We found that parents were primarily worried about physiological development issues," Abhinaya says. "For example, some parents were worried about VR damaging children's eyesight or children injuring themselves while using the apps."

"There were also concerns that children would interact with people online who would be a bad influence on them," says Anupam Das, co-

author of the paper and an assistant professor of computer science at NC State. "In terms of privacy, there were concerns that children might reveal too much information about themselves to strangers online."

"We found that parents did not seem too worried about data surveillance or data collection by the VR companies and app developers; they were more worried about risks of self-disclosure in social VR apps," Abhinaya says.

"VR technologies capture a tremendous amount of data on user movement, which can be used to infer information ranging from a user's height to medical conditions," Das says.

"VR technologies also capture a user's voice, and there are some concerns that voice recordings could be misused," Das says. "For example, it's possible that voice recordings might be manipulated with generative AI tools to create fake recordings. Only one parent was concerned about potential misuse of voice recordings."

"To be clear, most parents were aware of the possibility of data surveillance, but the vast majority were not concerned about it," Abhinaya says.

When it came to risk management strategies, the study found parents were having conversations with their children about being safe and not sharing personal information online. Many parents were also sharing VR accounts with their children, so that they could monitor their children's VR app use.

However, very few parents were making use of parental controls that were built into the VR technologies.

"Most parents were aware that the controls existed, they just weren't

activating them," Abhinaya says. "In some cases, parents felt their children were more tech-savvy than themselves, and wanted to give their kids autonomy regarding VR usage. This was particularly the case for teens. But in some cases, parents didn't make use of the controls due to technical challenges."

"In other words, some parents didn't know how to properly activate the controls," Das says. "There was also a desire for parental controls to incorporate additional features, such as a summary of what a child did while using a given app, who they interacted with, and so on."

The study found that parents felt they had the primary responsibility for protecting their children against risks associated with VR use. However, the parents also felt that VR companies should incorporate usable parental controls to help parents reduce risks.

In addition, parents felt policymakers should stay abreast of emerging technologies to create or modify laws and regulations that protect children online. Lastly, parents felt that schools have a role to play in teaching children how to navigate these new technologies safely.

"It is essential for parents to experience and understand VR before they let their children use it, to get a sense of the security and privacy risks VR may pose," Das says.

"However, while parents serve as the first line of defense for protecting children against these risks in VR, it is imperative for other stakeholders such as educators, developers, and policymakers to take proactive steps to ensure the comprehensive protection of children in VR environments."

The paper, "Understanding Parents' Perceptions and Practices Toward Children's Security and Privacy in Virtual Reality," will be presented at

the IEEE Symposium on Security and Privacy, being held May 20-22 in San Francisco, Calif. The paper was co-authored by Jiaxun Cao and Pardis Emami-Naeini of Duke University.

More information: Cao et al, Understanding Parents' Perceptions and Practices Toward Children's Security and Privacy in Virtual Reality (2024)

Provided by North Carolina State University