Did You Know?

Insights for XR App Developers

XR companies and developers are in a unique position to address users' privacy concerns. While XR programs require certain data to run, companies can control who has access to that data and how it is stored. Here's a guide directed at XR app developers on privacy considerations that they should be aware of.

Embedding Privacy into XR Design: When creating apps for XR, developers should consider embedding privacy considerations into the design principles of XR technologies across all stages of development, deployment, and operation. By integrating privacy into the core of XR systems from the outset, developers can proactively mitigate privacy risks before they emerge. This approach not only enhances user trust but also aligns with ethical standards, laying the groundwork for responsible and privacy-conscious XR implementation.

Privacy for Kids: XR developers should be aware of the unique concerns that arise with children and XR. Given their developmental phase, children may not fully understand the privacy risks posed by XR technologies, and the need for informed consent. The exposure of children's personal data poses serious immediate and long-term risks. In the wrong hands, children's data can potentially result in targeted manipulation or compromise their safety, making this group especially vulnerable compared to adults. Developers should consider implementing specific parental control mechanisms that enable parents to monitor which games their children can download on the device and limit the data third parties can request in-game.

Data Storage: Developers should be aware of where and how consumer data is being stored and who has access to it. For example, currently Apple's Vision Pro stores as much data as possible on its user's device without sharing it with third parties, while Meta stores user data on the Oculus cloud. Privacy-conscious consumers would be better off investing in a Vision Pro, and XR products which boast a similarly user-conscious data storage mechanism would likely be best suited for that market.

AI and XR Technologies: AI can play an important role in the development and use of XR apps. As such, developers should be aware of the risks that generative AI can expand the scope and nature of XR privacy concerns. Developers should use data sets to train their AI wherever possible, and when real-time data is required developers should ensure that their product is meeting privacy and ethics standards.

Working Together: Developers should work with and consult regulators regarding privacy in XR. They should also support the research and development of privacy-enhancing technologies that can be integrated into XR systems to better protect user data.

XR app developers play a pivotal role in shaping the future of privacy in digital environments and ensuring that privacy remains at the heart of innovation!