ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

700 K Street NW Suite 600
Washington, DC 20001

COMMENTS OF ITIF

Before the

National Institute of Standards and Technology, Department of Commerce

Washington, D.C.

In the Matter of:	)
Request for Comments Regarding Preliminary Research on Cybersecurity and Privacy Standards for Immersive Technologies	)

July 26, 2024

CONTENTS

Comments of ITIF 1
Introduction 2
Usability 3
Recommendations 4
Conclusion 5

INTRODUCTION

In the rapidly evolving landscape of immersive technologies, the integration of augmented and virtual reality (AR/VR)—immersive technologies that enable users to experience digitally rendered content in both physical and virtual space—is reshaping how users interact with digital environments. These technologies offer unprecedented opportunities for immersive experiences, from virtual meetings and interactive gaming to innovative educational tools and healthcare.

However, many AR/VR applications present unique cybersecurity and privacy concerns. These technologies collect large volumes of sensitive personal data, including a constant stream of data from users interacting with virtual environments. Much of the information that AR/VR devices collect is sensitive data not used in other consumer technology devices—yet it is critical to the core functions of AR/VR. For example, AR/VR devices may collect eye gaze and motion tracking data, which developers need to secure because the information users provide can directly reveal details they may expect to keep private, such as demographic information, where they live, or how they spend their free time. At the same time, developers must also ensure that the methods they use to protect user data doesn't also decrease the enjoyment or quality of the virtual experience. The unique challenges AR/VR technologies present, therefore, arise from the risks of aggregating sensitive information and the challenge of adapting security features designed for other consumer technologies into immersive, three-dimensional environments.[1]

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, non-partisan public policy think tank based in Washington, D.C., committed to articulating and advancing pro-productivity, pro-innovation, and pro-technology public policy agendas around the world that spur growth, prosperity, and progress. With these comments, ITIF primarily focuses on improving the usability of identity verification and authentication in AR/VR technologies because existing methods built for other technologies, such as personal computers or mobile devices, do not work well in immersive environments. NIST can play a critical role in building best practices and standards to best address these risks by leveraging technical expertise to analyze vulnerabilities in AR/VR systems and identify best practices for data security, building off of NIST's Cybersecurity Framework; expanding NIST's Digital Identity Guidelines to integrate user authentication securely into immersive platforms; developing guidelines for integrating biometric identity verification

[1] Ellysse Dick, "Balancing User Privacy and Innovation in Augmented and Virtual Reality," (ITIF, March 4, 2021), https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/.

methods securely into immersive platforms; and facilitating partnerships and collaborative efforts among stakeholders in the AR/VR ecosystem to address common security and privacy concerns collectively.

USABILITY

Usability refers to how easy a product is to use. Companies strive to improve the usability of their products to deliver a seamless and enjoyable experience to users. When it comes to AR/VR technologies, usability may reflect how intuitive, efficient, and satisfying an immersive experience is for the user, such as whether they can easily navigate a virtual environment or interact with virtual objects.[2] Usability enhances engagement by capturing the user's interest and creating an enjoyable experience.

Creating usable security features is essential to protect users because they are more likely to use security measures that are intuitive and unintrusive. For example, forcing users to use complex passwords can nominally improve security, unless those users start writing down these passwords on paper to remember them. Or installing locks on a door can make a building more secure, unless the individuals going in and out of the building find the lock so cumbersome that they start propping open the door.

One important step in creating usable security features for AR/VR technologies is authenticating users. Authentication is the process of confirming a user is who they claim to be, typically performed via credentials such as passwords, security questions, mobile devices, ID cards, or biometric data such as fingerprints, voiceprints, and facial features. The goal of authentication is to ensure only authorized users can access sensitive information or restricted services. Many online services use multifactor authentication to enhance security, such as requiring both a password and a biometric identifier, to ensure that even if attackers compromise a password, additional authentication requirements will prevent unauthorized access.[3]

One challenge with the shift to AR/VR technology is that the methods that work well for authenticating users in 2D digital spaces are more difficult to use with immersive technologies. For example, many people use password managers with their web browsers to manage a list of complex passwords to securely access online services, but AR/VR platforms have yet to effectively integrate password managers. As a result, users may be tempted to use simpler passwords that are more susceptible to attacks or find using AR/VR services too cumbersome. Traditional biometric authentication methods, such as fingerprint or face scans, are impractical because many devices, such as VR headsets, do not have fingerprint readers or cameras that can capture the necessary biometric information.[4] Finally, many online services use mobile phones to authenticate users, however, this method is also cumbersome and unfeasible since users cannot conveniently switch between their AR/VR headset and their phones.

As an additional challenge, compared with past technologies, AR/VR devices are in the "family computer" stage, in which households own a single device shared by all members. Thus, it is highly likely that an adult

---

[2] Mousa Al-kfairy, Ayham Alomari, Mahmood Al-Bashayreh, Omar Alfandi, and Mohammad Tubishata, "Unveiling the Metaverse: A survey of user perceptions and the impact of usability, social influence and interoperability, Heliyon, 2024, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11141377/.

[3] Dick, "Balancing User Privacy and Innovation in Augmented and Virtual Reality."

[4] David Moschella, "Slow Progress Is Taking the Fear Out of Artificial Intelligence," (ITIF, December 2, 2022), https://itif.org/publications/2022/12/02/slow-progress-is-taking-the-fear-out-of-artificial-intelligence/.

sets up these devices, and that an adult's account tends to be the primary account linked to the device that other household members use, regardless of age. Unless the adult has diligently created alternate accounts for other household members and assured that all household members effectively use their assigned accounts, anyone using the device will likely be able to access all the content available to the adult's primary account.

Newer forms of biometric authentication present a potential solution, as it is easier for consumers because they don't have to remember a password. Unlike passwords, biometric identifiers are impossible to share with another user. They are extremely difficult to forge, which makes them a more secure method of authentication than traditional passwords. Iris recognition is one potential solution for AR/VR technology that has seen some headway. Apple's Vision Pro headset uses iris scanning as identity verification, which eliminates the issue of children accessing adults' accounts and for multiple users to access the same device.[5]

Eventually, immersive technologies may also adopt new methods of authentication, such as zero-trust authentication. Zero-trust authentication relies on a series of questions based on a secret a user learns. For example, if the secret is "red AND round" they might answer yes to "apple?" but no to "fire truck?"[6]

RECOMMENDATIONS

Immersive technologies pose privacy and security risks that industry and government can address through the development of appropriate technical countermeasures. To assist in this effort NIST should:

- Leverage its technical expertise to analyze vulnerabilities in AR/VR systems and identify best practices for data security, building off of NIST's Cybersecurity Framework.[7]
- Expand NIST's Digital Identity Guidelines to integrate identity verification and authentication securely into immersive platforms with the understanding that users in the metaverse may want a digital presence separate from their real-life identity (as identified in the Digital Identity Guidelines SP 800-63A).[8]
- Develop guidelines for integrating biometric identity verification and authentication methods securely into immersive platforms to enhance user security and privacy.[9]
- Facilitate partnerships and collaborative efforts among stakeholders in the AR/VR ecosystem to address common security and privacy concerns collectively. NIST is well placed to convene experts across industry, civil society, and academia to best understand these issues and craft guidelines accordingly.

---

[5] Wayne Ma, "Apple's Mixed Reality Headset to Offer Iris Scanning for Payments, Logging In," *The Information*, October 14, 2022, https://www.theinformation.com/articles/apples-mixed-reality-headset-to-offer-iris-scanning-for-payments-logging-in.

[6] Juan Londoño, "User Safety in AR/VR: Protecting Adults," (ITIF, January 17, 2023), https://itif.org/publications/2023/01/17/user-safety-in-ar-vr-protecting-adults/.

[7] *NIST*, "Cybersecurity Framework," accessed on 06/20/2024, https://www.nist.gov/cyberframework.

[8] *NIST*, "Digital Identity Guidelines," accessed on 07/02/2024, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

[9] Dick, "Balancing User Privacy and Innovation in Augmented and Virtual Reality."

CONCLUSION

Immersive technologies are already transforming the ways in which users interact with each other, creating highly engaging and personalized experiences. As users continue to construct digital identities within these environments, the volume and sensitivity of the data collected will significantly increase, creating more threats to users' privacy and security. Therefore, digital identity should play a key role in shaping the governance structures in immersive technologies and NIST is well placed to lead this charge.

Thank you,

Alex Ambrose
Policy Analyst, ITIF