ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

700 K Street NW Suite 600
Washington, DC 20001

COMMENTS OF ITIF

Before

Standards Australia

In the Matter of:	)	DR AS 5402:2024
Children's Safety in the Metaverse	)	

January 24, 2025

CONTENTS

INTRODUCTION AND SUMMARY

Improving children's online safety is currently a global priority, with policymakers proposing legislation to address issues spanning child exploitation, privacy, age-appropriate design, and age verification. Ensuring young people get the best possible online experience—balancing safety with utility—is difficult considering every child and teenager has different needs and faces unique circumstances.

On top of these broader concerns, properly addressing the risks children face with immersive technologies is even more challenging. Most existing immersive technologies are not made for children under 13, yet as *Standards Australia* research finds, two-thirds of metaverse users are under the age of 16.[1] Children explore spaces designed for adults, which leads to exposure to age-inappropriate content and can build harmful habits and behaviors in children's mental and social development.

Addressing these risks will require a combination of market innovation and thoughtful policymaking. Companies' design decisions, content moderation practices, parental control tools, and trust and safety strategies will largely shape the safety environment in the metaverse. However, public policy interventions are necessary to tackle certain safety threats.

The stated objective of DR AS 5402:2024, "Children's Safety in the Metaverse," is to provide a practical framework for advancing children's safety in the metaverse by providing guidance for industry, policymakers, educators, parents and guardians, and children. The draft standards focus on children's safety, privacy, and accessibility in the metaverse.[2]

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

[1] "Virtual fight for kids' safety: Standards Australia releases landmark draft standard to protect children in the Metaverse," *Standards Australia*, December 3, 2024, https://www.standards.org.au/news/virtual-fight-for-kids-safety-standards-australia-releases-landmark-draft-standard-to-protect-children-in-the-metaverse.

[2] "Children's safety in the metaverse," *Standards Australia*, 2024, https://comment.standards.org.au/Drafts/8bf445cd-064c-44ab-a9f1-162e5576870a.

progress. With these public comments on the draft standards, ITIF argues first, Standards Australia should establish age-based guidelines for the metaverse using existing content ratings; second, require device operating systems to create an opt-in "trustworthy child flag" system; third, work with global, government-led groups to build voluntary industry standards for the metaverse with a focus on interoperability; and fourth, promote digital literacy campaigns, such as those overseen by the eSafety Commissioner, to educate children on how to operate in the metaverse safely.

COGNITIVE DEVELOPMENT IN THE METAVERSE

Cognitive development refers to the changes that occur in children's mental abilities as they grow and mature, such as attention, language, learning, and thinking. Since many children spend a lot of time on screens, researchers have begun to investigate screens' impact on children's development and cognitive skills, such as memory, attention, and spatial cognition.[3] However, much of the current discourse centers on screens' impact in taking attention away from children. When these screens become the avenue for immersive experiences, more questions arise as to how attention and cognition are impacted through augmented and virtual reality (AR/VR) experiences. If children are less able to distinguish between what is real and what is imaginary compared with adults, children may confuse fictional immersive experiences with real ones. Confusion between reality and imagination is a normal part of child development, but questions remain whether AR/VR technologies will exacerbate this confusion and therefore hinder cognitive development.[4]

Children are also more likely than adults to share personally identifiable information (PII) on the Internet. A child's comprehension of privacy increases as they get older, but this understanding does not always translate to the online world.[5] For example, children can learn to understand real-world privacy concerns, such as safeguarding their home address or the significance of closed doors, but they may not understand the implications to their privacy of participating in online voice chats or sharing digital photos.[6]

Another typical aspect of child development is building parasocial relationships. Typically described as a one-sided, emotional attachment to a fictional character, some studies have shown children and adolescents often utilize parasocial relationships to help form their identity.[7] The line can become more blurred for children through social realism, or believing a fictional character exists in the real world. Children's gravitation toward

[3] Polyxeni Kaimara, Andreas Oikonomou, and Ioannis Deliyannis, "Could virtual reality applications pose real risks to children and adolescents? A systematic review of ethical issues and concerns," National Library of Medicine, accessed on May 8, 2024, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8328811/.

[4] Ibid.

[5] Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri, "Children's data and privacy online: Growing up in a digital age," *London School of Economics*, December 2018, https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf.

[6] Allen St. John, "Warning Kids About Digital Privacy Doesn't Work. Here's What Does," *Consumer Reports*, August 28, 2018, https://www.consumerreports.org/electronics-computers/privacy/kids-and-digital-privacy-what-works-a7394637669/.

[7] Angela Haupt, "In Defense of Parasocial Relationships," *Time*, July 23, 2023, https://time.com/6294226/parasocial-relationships-benefits/.

attachment and building parasocial relationships may be heightened in virtual experiences compared with the characters and individuals in the real world.[8]

For example, the relationships a child has with virtual characters may become more complex if those characters perform harmful actions or harass the child, with the child developing unhealthy behaviors offline because of their attachment to and interactions with the characters.[9] In addition, these relationships could be harmful if companies use them to advertise products or services to the child that are not age appropriate. These digital characters may use emotion recognition, or technology's ability to identify human emotions from facial expressions, voice inflections, body language, and other physical signals, in order to grow further connections with users.[10] Therefore, the government should further examine how children build these relationships, particularly as it relates to the use of emotion recognition.[11]

Though not included in the government recommendation section, the draft guidelines rightfully highlight that a possible solution to developmental considerations is to establish age-based guidelines for the metaverse by using existing content ratings, a strategy that has worked for traditional media. The Australian Classification Board assigns ratings and content warnings to movies, computer games, and certain publications before they can be released in Australia, which allow users to be aware of content that might trigger any sensibilities.[12] While such a standard is more challenging to implement in immersive technologies—given user experiences unique to the metaverse like live chats and translations, the scope and scale of user-generated content, and the cross-platform nature of immersive experiences—platforms may opt to implement a categorization or tagging system like those seen in platforms such as YouTube, which will provide appropriate labeling of worlds depicting violence or sensitive content.[13]

AGE-APPROPRIATE CONTENT

Because children and adults both populate shared immersive spaces, identity and age verification will play a crucial role in making sure the users who interact with children are also children. But identity verification for

[8] Melissa N. Richards and Sandra L. Calvert, "Measuring young U.S. children's parasocial relationships: toward the creation of a child self-report survey," *Journal of Children and Media*, April 7, 2017, https://cdmc.georgetown.edu/wp-content/uploads/2012/08/Richards-Calvert-2017.pdf.

[9] Jakki O. Bailey et al., "Virtual reality's effect on children's inhibitory control, social compliance, and sharing," *Journal of Applied Developmental Psychology*, *Volume 64*, July-September 2019, https://www.sciencedirect.com/science/article/abs/pii/S0193397318300315#.

[10] Kaitlin L. Brunick et al., "Children's future parasocial relationships with media characters: The age of intelligent characters," *Journal of Children and Media*, 10:2, 181–190, https://cdmc.georgetown.edu/wp-content/uploads/2016/04/Brunick-et-al-2016.pdf.

[11] Ibid.

[12] "What are the ratings?," *Australian Government Department of Intrastructure, Transport, Regional Development, Communications and the Arts*, retrieved on January 21, 2025, https://www.classification.gov.au/classification-ratings/what-are-ratings.

[13] 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/; Alex Ambrose, "User Safety in AR/VR: Protecting Kids," (ITIF, September 3, 2024), https://itif.org/publications/2024/09/03/user-safety-in-ar-vr-protecting-kids/.

children is nuanced and complex. There are multiple ways online services can verify users' ages, and each of these methods comes with different strengths and weaknesses. Some are more accurate but more invasive, whereas others are less invasive but also less accurate.

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 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. Therefore, single shared devices can make it easier for children to skirt age-restricted content and engage in areas of immersive experiences not suitable for their age.

Before the passage of any age verification laws, many online services, including adult websites and social media platforms, required users to either check a box indicating that they were over a certain age or input their date of birth to confirm they were over a certain age. This form of self-verification is the least invasive because it only requires users to disclose, at most, one piece of personal information: their date of birth. Because many people share the same birthday, this piece of information cannot uniquely identify an individual. However, this method is also the least reliable, as underage users can and often do lie about their age in order to gain access to certain online services.[14]

Consequently, account sharing erodes the effectiveness of parental controls offered by hardware and software developers. For example, parents might set screen time limits, restrict access to apps, or restrict children's ability to add someone to their friends list without prior authorization. However, if children have access to the primary adult account, they can alter parental controls. The prevalence of account sharing in AR/VR devices makes age-gating AR/VR more difficult without using facial recognition or other age-validation tools. This underscores the challenges parents face in monitoring and regulating their children's use of AR/VR technology, while also empowering children to have autonomy over their time online.

Furthermore, most age verification laws require providing a government-issued ID to prove a user's age. In real-world instances of age verification, consumers typically show ID to a bartender or cashier to purchase alcohol or cigarettes. Online, however, a user typically turns over their ID to the online service, which then may be stored by the platform.

Digital forms of government-issued identification could solve some of the privacy concerns associated with ID checks for age verification, as well as make the process more efficient, but most children lack government-issued identification. Online ID checks typically require users to upload a photo of their physical ID as well as sometimes go through additional steps to prove the ID belongs to them, such as uploading a current image of their face to compare to the photograph on the ID. Therefore, requiring platforms to have users verify their age through uploading government-issued ID would exclude many children who are old enough to use these platforms from accessing them. If designed right, digital IDs would streamline this process and allow users to

[14] Ash Johnson, "How to Address Children's Online Safety in the United States," (ITIF, June 3, 2024), https://itif.org/publications/2024/06/03/how-to-address-childrens-online-safety-in-united-states/.

only share necessary information. For example, individuals trying to access an age-restricted online service could verify that they are over a certain age without providing their exact date of birth, let alone all the other information a physical ID would reveal.

Another potential method of age verification is using artificial intelligence (AI) to estimate a user's age from an image of their face. Combined with privacy protections requiring online services to delete users' images after the age estimation process is complete, this would minimize the amount of personal information users have to give up in order to verify their age. Of course, age estimation technology is not perfectly accurate and likely never will be—no form of age verification is—but it is constantly improving. In 2023, age estimation provider Yoti reported that the company's technology could accurately estimate 13- to 17-year-olds as under 25 with 99.93 percent accuracy and 6- to 11-year-olds as under 13 with 98.35 percent accuracy, with no discernable bias across gender or skin tone. Yoti's mean absolute error—the average error the technology makes when estimating an individual's age—is 1.3 years for children ages 6 through 12 and 1.4 years for teenagers ages 13 through 17. Therefore, there is high reliability of keeping 6-year-olds out of spaces designed for teenagers, but less reliability differentiating between 12- and 13-year-olds.[15]

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.[16]

In the metaverse, without proper identity verification, bad actors can pose as children or trustworthy figures, making it easier to gain a child's trust. As in the real world, criminals can manipulate this trust to groom, exploit, and abuse children. For example, bad actors can threaten and coerce a child into creating sexually explicit content of themselves, or the bad actor's avatar could commit sexual abuse toward the minor.[17] If the immersive experience contains a haptic device, the bad actor could use that technology to make the experience feel more "real." In other words, the immersive nature of these experiences can cause people to feel the potential emotional and traumatic aftermath more acutely because they believe their real physical body is threatened alongside the virtual body.[18] Children who come from vulnerable populations, suffer from poor mental health, or have poor parental or guardian relationships are even more susceptible to this abuse.[19]

---

[15] Ash Johnson, "How to Address Children's Online Safety in the United States."

[16] Alex Ambrose, "Comments Before NIST Regarding Preliminary Research on Cybersecurity and Privacy Standards for Immersive Technologies," (ITIF, July 26, 2024), https://itif.org/publications/2024/07/26/comments-before-nist-regarding-research-cybersecurity-privacy-standards-immersive-technologies/.

[17] "Metaverse: A Law Enforcement Perspective," Interpol, January 2024, https://www.interpol.int/en/News-and-Events/News/2024/Grooming-radicalization-and-cyber-attacks-INTERPOL-warns-of-Metacrime.

[18] Nelson Reed and Katie Joseff, "Kids and the Metaverse," *Common Sense Media*, accessed on May 22, 2024, https://www.commonsensemedia.org/sites/default/files/featured-content/files/metaverse-white-paper.pdf.

[19] Sameer Hindjua, "Child Grooming and the Metaverse—Issues and Solutions," *Cyberbullying Research Center*, accessed on May 22, 2024, https://cyberbullying.org/child-grooming-metaverse.

Furthermore, as the draft standards rightfully address, anonymous online identities are important too, as some users may opt not to use their real name or image in their online profiles in order to access and interact with online groups they would be unable to safely interact with in the real world. Children should be free to shape their own digital identities, with the creativity and flexibility for their online personas to reflect whatever parts of their identity they choose outside their parents' and guardians' interests and to develop their identity and personality on their own terms.

Instead of social media bans, Australia should pursue regulations that allow platforms to assume everyone is an adult unless they have been marked as a child.[20] This could be done through a "child flag" in a device's operating system that allows parents to easily access the same device as one being used by a minor. Websites and apps that deliver age-restricted content could then check whether a device or account on a device has received the flag and, if called for, block a user from seeing the content. By implementing this opt-in, largely voluntary system, users would not face the same disruptions caused by a blanket age-gate mandate.

SUPERVISION

The best approach to parental controls allows children and their parents to tailor kids' online experience in a way that is best suited to each child's individual needs, striking a good balance between government involvement, platform responsibility, and parental choice. Standards should avoid requiring online services to default to the strictest settings for minors' accounts strips away some of this choice and would likely result in many minors missing out on potentially beneficial design features—such as algorithmic recommendation systems—if they, like many users, stick with the default options rather than personalize their account settings.[21] It would be more beneficial for certain features that are most important for safety, such as restricting who can message minors and view their profiles, to be left on by default while other features, such as screen-time limits and personalized recommendation systems, are left in the hands of parents. Conversely, relying only on parental controls requires parents to be highly involved and technologically literate, which is not feasible in every situation.[22]

As the draft rightfully asserts, Standards Australia can establish a government-led forum to create a voluntary industry standard for interoperability on cross-platform parental controls, which would enable parents to create universal limits on their children's online behavior across multiple devices.

EDUCATIONAL INITIATIVES

Children may encounter immersive technologies in educational contexts—and not just at school but also with educational apps and at libraries and museums.[23] In fact, AR/VR experiences can engage students in hands-on, gamified approaches to learning in a variety of subjects, which have been shown to support cognitive

[20] Ash Johnson and Alex Ambrose, "Social Media Ban for Children Is a Step Backward for Australia," (ITIF, November 19, 2024), https://itif.org/publications/2024/11/19/social-media-ban-for-children-is-a-step-backward-for-australia/.

[21] Alan McQuinn, "The Economics of 'Opt-Out' Versus 'Opt-In' Privacy Rules" (ITIF, October 6, 2017), https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules/.

[22] Ash Johnson, "How to Address Children's Online Safety in the United States."

[23] Todd Richmond, "Experience History and Art in a Whole New Way with AR and VR in Museums," *IEEE Transmitter*, October 11, 2019, https://transmitter.ieee.org/ar-vr-in-museums/.

development and increase classroom engagement.[24] These technologies expand the possibilities of learning environments by enabling exploration outside the bounds of physical space, such as teaching life science skills by placing students inside virtual intestines or watching a Shakespeare play from inside a virtual Globe Theatre, and enhancing collaboration and hands-on learning.[25] They also provide new tools for children with learning and physical disabilities to engage with their teachers and their school content. Given the slow rate of consumer adoption, however, many kids' first exposure to AR/VR technologies could be in classroom settings, which also is consistent with existing trends in digital literacy; teachers are the primary source of knowledge for key information and communications technology skills.[26] Governments should provide funding to schools and public libraries for digital literacy campaigns that teach children how to be safe online and parents how to keep their children safe online, including safe AR/VR use and the potential ways the threats present in the 2D Internet might materialize in online immersive environments.

CONCLUSION

In the wake of Australia's parliament banning social media for children under 16—the very same age group driving the adoption of immersive technologies—it is promising Standards Australia is looking to build standards driving safe experiences for immersive technologies.[27] Standards Australia should establish age-based guidelines for the metaverse using existing content ratings; require device operating systems to create an opt-in "trustworthy child flag" system; work with global, government-led groups to build voluntary industry standards with a focus on interoperability; and promote digital literacy campaigns for children to operate in the metaverse safely. These draft standards provide a great overview of the issues present for children when interacting in the metaverse, and Standards Australia should continue to drive standards development in this important arena.

Thank you for your consideration.

Alex Ambrose
Policy Analyst, Information Technology and Innovation Foundation

---

[24] Ellysse Dick, "The Promise of Immersive Learning: Augmented and Virtual Reality's Potential in Education" (ITIF, August 30, 2021), https://itif.org/publications/2021/08/30/promise-immersive-learning-augmented-and-virtual-reality-potential/.

[25] Nick Clegg, "New Education Product for Quest Devices Will Help Teachers Bring Subjects to Life in New Ways," *Meta*, April 15, 2024, https://about.fb.com/news/2024/04/new-education-product-for-quest-devices/; Nick Clegg, "How the Metaverse Can Transform Education," *Meta*, April 12, 2024, https://nickclegg.medium.com/how-the-metaverse-can-transform-education-20ed9d355b5f.

[26] Ellysse Dick, "The Promise of Immersive Learning: Augmented and Virtual Reality's Potential in Education."

[27] Ash Johnson and Alex Ambrose, "Social Media Ban for Children Is a Step Backward for Australia" (ITIF, November 19, 2024), https://itif.org/publications/2024/11/19/social-media-ban-for-children-is-a-step-backward-for-australia/; Nelson Reed and Katie Joseff, "Kids and the Metaverse," *Common Sense Media*, accessed on January 24, 2025, https://www.commonsensemedia.org/sites/default/files/featured-content/files/metaverse-white-paper.pdf.