ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

User Safety in AR/VR: Protecting Kids

ALEX AMBROSE | SEPTEMBER 2024

Children play a crucial role in driving adoption of immersive technologies—and parents, corporations, and regulators all have roles to play in balancing privacy and safety concerns to ensure they can enjoy safe, engaging, and innovative experiences.

KEY TAKEAWAYS

- Ensuring that 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.
- Play, imagination, and creativity are all critical for children's development. Immersive technologies can be beneficial in those regards by fostering social connection and stimulating creativity and imagination.
- The metaverse is not designed for young people, per se, yet they are the technologies' main adopters. This enthusiasm—and their already overwhelming use of immersive gaming apps—indicates kids will drive the market for AR/VR technologies.
- Companies' design decisions, content moderation practices, parental control tools, and trust and safety strategies will largely shape the safety environment in the metaverse.
- Bills such as the Kids Online Safety and Privacy Act may lead regulators to over-censor content on AR/VR platforms or lead the platforms themselves to censor more content than necessary to avoid liability.
- Children's online safety legislation for AR/VR should instead balance personal, parental, corporate, and government responsibility—for example, by requiring device operating systems to create an opt-in "trustworthy child flag" for user accounts.

CONTENTS

INTRODUCTION

Improving children's online safety is currently a global priority, with policymakers proposing legislation spanning child exploitation, privacy, age-appropriate design, and age verification. Many critics claim that the Internet, and particularly social media, is responsible for a vast array of potential harms to younger users—including, but not limited to, bullying, addiction, sexual exploitation, and poor physical and mental health outcomes such as depression, body image disorders, self-harm, and lack of physical activity and exercise. For example, in June 2024, U.S. Surgeon General Vivek H. Murthy called for labeling social media as being dangerous as tobacco or alcohol.[1] Others reject these broad claims, noting that they are not backed up by the scientific literature. They note that the Internet and social media can have positive effects on young lives, such as connecting them with entertainment, education, and community. However, 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. Therefore, many still call for interventions to make online spaces better for children, such as improving digital and media literacy, developing better cross-platform parental controls, and increasing funding for law enforcement to investigate crimes against children online.[2]

However, these conversations about online safety often overlook augmented and virtual reality (AR/VR) technologies. Immersive technologies foster social connection and stimulate creativity and imagination. Play, imagination, and creativity are all imperative for children to develop.[3] But properly addressing the risks children face with immersive technologies is a challenge. Most existing immersive technologies are not made for children under 13. Children explore adult-designed spaces, 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.

Policymakers are already addressing children's safety on "2D" platforms such as social media, leading to regulations that may affect AR/VR tech. Before enacting these regulations, they should consider AR/VR developers' ongoing safety efforts and ensure that these tools maintain their effectiveness. When safety tools are insufficient, policymakers should focus on targeted interventions to address proven harms, not hypothetical risks.

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.

This report is part of a series that explores user safety challenges in AR/VR technologies among three specific demographics: adults (ages 18 and older), teens (ages 13 to 17), and children (ages 12 and below).[4]

This report offers the following policy recommendations:

- Congress should pass comprehensive federal privacy legislation.[5]
- The U.S. House should not pass the Kids Online Safety and Privacy Act (KOPSA).
- Congress should pass legislation requiring device operating systems to create an opt-in "trustworthy child flag" for user accounts.
- Congress should pass legislation establishing a government-led forum to create a voluntary industry standard for interoperability on cross-platform parental controls.
- Congress should pass federal legislation similar to the Coogan Act and Illinois's child influencer legislation that protects child performers online.
- Congress should provide funding for digital literacy campaigns that teach children how to be safe both online and when using AR/VR devices.
- Congress should provide funding for research on the long-term physical health impacts and developmental implications of AR/VR devices.
- The National Institute of Standards and Technology (NIST) should build on its Digital Identity Guidelines with additional recommendations for integrating biometric identity verification methods securely into immersive platforms.[6]

THE UNIQUE CONTEXT OF CHILDREN'S AR/VR USE

Generation Z and Generation Alpha—people born between 1997 and 2024—are innate adopters of technology, with technology being an integral part of their lives starting in their childhoods. According to Common Sense Media, 70 percent of children ages 8–17 are interested in experiencing VR, while 17 percent report owning a headset. The metaverse is not designed for young people, yet they are the main drivers of the technology.[7] This enthusiasm from kids—and their already overwhelming use of immersive gaming applications—indicates that they will be the drivers of the market for AR/VR technologies.[8]

It is imperative that children have the space to play, imagine, and create as part of their development because it is through play that they learn about themselves and the world around them. Children have used toys and technologies throughout history to create and play.[9] They develop social and cognitive skills through pretend play and gaming activities. Through role-playing, children work out confusing, scary, or new experiences. AR/VR provides novel opportunities for children to continue cultivating these experiences and grow alongside the technology. As such, the current state of adoption for children mostly centers on gaming and education, coupled with parents' role in overseeing their children's AR/VR use.

The Current State of Adoption

AR/VR applications span industries such as manufacturing, medicine, and education. However, most consumer adoption of AR/VR is primarily found in gaming. Sixty-five percent of Americans play video games at least one hour a week, while 76 percent of children under 18 say they play video games.[10] VR headsets are currently the least utilized device for gaming, with mobile and consoles being more popular.[11] In addition, outside gaming contexts, most consumers have not yet integrated AR/VR technology into their day-to-day routines.[12]

VR headsets have been on the consumer market since the mid-1990s, but it wasn't until the mid-2010s that VR headsets started to gain popularity. One of the earliest headsets, the 1995 Nintendo Virtual Boy, sold only 770,000 total units, leading Nintendo to discontinue the product. But Apple's Vision Pro headset, which went on sale on January 19, 2024, sold 200,000 units in just its first 10 days.[13] Despite this clear growth in interest, AR/VR devices are currently in the "family computer" stage in which households own a single device shared by all members, unlike smartphones whereby each family member has their own. Thus, most households share a single account, often tied to the adult purchaser of the device.

AR/VR Gaming

For children and adults alike, gaming is the most popular use of AR/VR technology. Games such as Minecraft, Roblox, and Fortnite are extremely popular with children under 13. These sandbox games—open-concept games often without objectives and fueled by individual creation—allow children to act on original ideas, explore, and construct.[14] Furthermore, children often use games to make friends and communicate.[15]

But, there exists a gender imbalance for children who game, as boys often integrate their game preferences and status as a "gamer" into their daily lives more so than girls do, who often face larger hurdles overcoming shame with their gaming identity.[16] According to the Digital Wellness Lab, 40 percent of boys play video games every day but only 10 percent of girls say the same.[17] This disparity suggests that while gaming is a significant part of children's lives, the experiences and safety levels can vary greatly between genders. Understanding these dynamics is crucial for developing inclusive, supportive, and safe immersive environments for all children as AR/VR technology becomes more integrated in daily life—in gaming and outside gaming. In addition, the historic exclusion of women and girls in gaming poses a challenge to the industry that needs to be addressed, as platforms can use gender inclusion to expand their audience and increase market potential.[18]

Balancing Parental Control and Children's Autonomy

Children under 13 do not meet the age requirement for most social media platforms, yet 56 percent of U.S. children have their own social media accounts.[19] Many parents today create accounts for their children, documenting their existence before the child is even born; a child's first photograph online is often of them in the womb. In addition, influencers, or users who become famous through social media and use their celebrity to endorse and promote products, are becoming an increasingly important sector of the digital economy. "Kidfluencers," or kid influencers, are children under the age of the platforms' terms of service yet have well-known social media presences themselves. They are a growing demographic on social media platforms, with most of these accounts run and managed by children's parents.[20] In a 2023 Morning Consult poll, 57 percent of Generation Z children said they would become an influencer if given the opportunity.[21]

Even though AR/VR technology remains at the "family computer" stage, it is important for children themselves to have a voice in shaping their own online experiences, exploring their own interests, and fostering independence for their online futures. 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.[22] 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 quickly alter parental controls (unless parents ensure their accounts are password protected).[23] 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.[24] 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.

Even though AR/VR technology remains at the "family computer" stage, it is important for children themselves to have a voice in shaping their own online experiences, exploring their own interests, and fostering independence for their online futures.

As such, children's online habits are typically a reflection of the habits of their parents and guardians. Parents often see themselves as the source of positive digital role modeling, and some studies conclude that children are less likely to engage in problematic social media use such as prolonged time online when their parents are tolerant and supportive of their time online.[25] Parents can use parental controls such as screen time limits and prompts for breaks. At the same time, not every child lives in a home with parents willing or able to look out for their best interests online. Even parents who have the time and skills to monitor their children's use need tools to make that easier or, in some cases, possible. Therefore, any effective guardrails should balance personal, parental, corporate, and government responsibility.[26]

Education and AR/VR

Children may encounter immersive technologies in educational contexts—and not just at school but also with educational apps and at libraries and museums.[27] 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 development and increase classroom engagement.[28] 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.[29] They also provide new tools for children with learning and physical disabilities to engage with their teachers and their school content.[30] 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.[31]

However, a lack of tech adoption—further worsened by some districts' budget constraints—means there is no unified use of immersive technologies across the United States.[32] In addition, there is a lack of plans for sustained and expanded use of technology in schools. Certain districts have sustainability plans for when existing technology ages out or the devices no longer work, but many educators are not planning for this problem.[33] Again, education is an arena for emerging technologies to thrive, as long as policies balance parental and educator concerns, children's best interests, and government responsibility.

OVERVIEW OF CURRENT THREATS FOR ALL USERS OF AR/VR TECHNOLOGY

Previous Information Technology and Innovation Foundation (ITIF) research has summarized various threats for adult and teenage users of AR/VR technology.[34] As this report highlights, the immersive nature of AR/VR technology and its potential pairing with haptic technology—wearable technology that uses sensors to create tactile experiences alongside the immersive experience, such as gloves or joysticks—could bring new safety challenges that are not present in devices with 2D screens. Table 1 illustrates the threats to safety identified in previous reports.

Table 1: Summary of known threats and potential responses[35]

Type of Threat	Where It Occurs	Potential Solutions
Distracted driving, biking, or walking	Most augmented reality devices	▪ Car mode; Focus mode: reduce notifications from non-navigation apps
Motion sickness	Virtual reality devices	▪ Customizable movement and camera settings: camera rotation angle, camera rotation speed, vignette/tunnel vision mode, smooth movement versus teleport movement

Type of Threat	Where It Occurs	Potential Solutions
Obscured or limited field of view	Most extended reality devices	▪ Establishment of digital boundaries, such as the "guardian" system ▪ Alert systems for instances when humans or objects trespass virtual boundaries ▪ Pop-ups and notifications before the use of apps
Stalking and "swatting"	Extended reality devices	▪ Cybersecurity investment ▪ Technological literacy campaigns for users ▪ Pop-ups and warnings about sharing sensitive information when livestreaming ▪ Privacy and data stewardship standard setting ▪ Federal privacy legislation
Leading users to dangerous or off-limits locations	Augmented reality	▪ Geofencing ▪ Robust reporting system ▪ Conscious product design that is mindful of hazardous areas
Incitation of violence or vandalism	Multi-user immersive experiences	▪ Content moderation tools: flagging system, content removal, product throttling
Health misinformation	Multi-user immersive experiences	▪ Content moderation tools: flagging system, content removal, pop-up systems
Sexual violence with immersive haptics	Sex-related extended reality haptic devices	▪ User-driven responses: confirming the identity of the other user before using immersive haptics
Sexual violence	Multi-user immersive experiences	▪ Personal safety tools for users: mute, block, report, and "safe zone" functionality ▪ Establishment of personal boundaries or space bubbles, which prevent other avatars from violating a user's personal space ▪ Content moderation by platforms or community leaders
Cyberbullying and virtual harassment	Multi-user immersive experiences	▪ Personal safety tools for users: mute, block, report, and "safe zone" functionality ▪ Decentralized content moderation: community-driven moderation through world/room moderators ▪ Legislation that codifies cyberbullying as a crime

Type of Threat	Where It Occurs	Potential Solutions
Harmful content	Multi-user immersive experiences	▪ Traditional content moderation tools: pop-ups, automated flagging systems ▪ Decentralized content moderation: community-driven moderation through world/room moderators
Addiction and psychological impact of virtual socialization	Multi-user immersive experiences	▪ User-established screen time restrictions, screen time reports ▪ Pop-ups notifying users of extended use of device/platform ▪ Content moderation tools ▪ Appropriate categorization of content: Entertainment Software Rating Board ratings, mature/adult tags in-platform
Gambling	Multi-user immersive experiences, extended reality devices	▪ ID verification: if not possible on-device, through the use of a companion app ▪ In-app resources for those facing gambling addiction
Identity theft, fraud, and ransomware	Multi-user immersive experiences	▪ Two-factor authorization ▪ Restricting player-to-player item transfers ▪ Integration of password managers ▪ Adoption of passwordless technology such as Zero-Trust Authentication
Impersonation and reputational damage	Multi-user immersive experiences	▪ Impersonation report systems ▪ Locking photorealistic avatars function for non-verified users

As consumers use immersive technologies more, policymakers should consider the new safety challenges these technologies may introduce. For example, earlier in 2024, Apple released the Apple Vision Pro, signaling a major drive toward consumer-grade AR/VR products and applications. After the release, however, there were incidents that raised physical safety concerns, such as users driving or walking while wearing the headset.[36] Even though user manuals warn against such behavior, these incidents highlight physical safety concerns present in immersive technologies that, while not novel, are extensions of safety issues present in technology today. For example, despite laws against it, many people use their cell phone while driving—doing so while wearing a headset is an extension of pre-existing safety concerns. AR/VR technologies will present novel safety harms, but they also need to better address many pre-existing safety harms.

UNIQUE THREATS FOR KIDS IN AR/VR TECHNOLOGY

Certain threats such as virtual harassment, addiction, gambling, and impersonation can affect all users of AR/VR technology, but there are some unique ways children can be impacted within these issue areas. Understanding how children are particularly at risk is vital for improving these platforms and systems for developers and policymakers alike.

Sexual Predation

There are several existing laws protecting children from abuse, neglect, exploitation, and physical harm both in the real world and the digital world. Many laws and proposals related to children's online safety center protections around child sexual exploitation.[37] Children can encounter sexually exploitative experiences online, such as simulated sex acts or rape threats. According to a 2021 study, approximately 34 percent of 18- to 20-year-old respondents had been asked to do something sexually explicit online as a child.[38]

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 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.

In the United States, multiple states have passed or considered legislation that would restrict children under a certain age from accessing certain online services without parental consent, or at all.[39] Some of these laws—in Arkansas, Louisiana, Mississippi, Texas, Utah, and Virginia—target online services that provide adult content. Others—introduced in Pennsylvania and Wisconsin and passed in Arkansas, Connecticut, Louisiana, Ohio, and Utah—target social media platforms.[40] As of July 2024, 19 U.S. states have passed age verification laws.[41]

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.[42]

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. As the United States still does not have a federal data privacy law, this system remains on a case-by-case basis depending on the policies of the platform.[43]

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 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.[44] 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.

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.[45] 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.[46] 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.[47] 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.[48]

Exposure to Inappropriate Content

In addition to sexual predation, children are susceptible to exposure to inappropriate and sexual content in the metaverse because the environment is not created for children alone. Exposure to sexual content, such as pornography, at a young age has been shown to lead to a greater acceptance of sexual harassment and sexual aggression.[49] According to one American Psychological Association report, the average age of boys' first exposure to pornography is about 13 years old. In a 2023 Common Sense Media survey, 15 percent of teen respondents said their first exposure was before the age of 10.[50]

There is inappropriate content or content that is potentially harmful to children on the Internet and on social media, just as there is in any form of media. This may include adult content, bullying, hate speech, and depictions or promotion of self-harm, suicide, eating disorders, substance abuse, or violence. Most of these forms of content violate most online services' community guidelines, and most online services work diligently to remove harmful content, but the sheer amount of content online means that some of it will inevitably slip through the cracks in content moderation. Online services that do allow adult content typically have restrictions in place meant to ensure that only adult users seeking out such content are exposed to it, or offer alternative versions of their services targeted at a younger audience. Adults have a legal right to access sexually explicit content, so gatekeeping access to adult online services is different from gatekeeping access to social media.[51]

Assigning age ratings to content is another strategy that has worked for traditional media. The Motion Picture Association assigns ratings that reflect a film's content, considering elements such as violence, profanity, depictions of substance use, and sexual content. Additionally, content warnings such as the ones established by the Entertainment Software Rating Board allow users to be aware of content that might trigger any sensibilities. While such a standard is more challenging to implement in immersive technologies, 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.[52]

Regulations should allow platforms to assume everyone is an adult unless they have been marked as a child, a process that should be easy and accessible.

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. Yet, current social media regulation is seemingly reliant on each child having their own device. Biometric-based identity verification, such as Apple's iris recognition on Vision Pro devices, is one potential solution if it reliably prevents impersonation.

Regulations should allow platforms to assume everyone is an adult unless they have been marked as a child, a process that should be easy and accessible. This could be done through a "child flag" in a device's operating system that allows parents to a 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.[53]

Cyberbullying and Virtual Harassment

As in the real world, children in the metaverse are subject to bullying. Outside cyberbullying—such as name-calling or verbal abuse on voice and text chats—children can also experience virtual assaults such as punching or kicking when using avatars.[54] Children's mental health has been another major concern for policymakers and parents who are worried about the potential adverse effects social media can have on young users.[55]

Concerns over cyberbullying and harassment continue to loom on metaverse platforms, as some of them have already struggled with tackling harassment. For example, Meta's Horizon Worlds instituted a "bubble" boundary around users' avatars to prevent virtual assaults by not allowing avatars to get within a certain proximity of each other because of repeated instances of avatars assaulting other users.[56] Moreover, when one user experimented as a 13-year-old girl on VRChat, "almost immediately" the user was inundated with sexual comments.[57] Currently, AR/VR experiences' user base tends to be from the gaming community, an online demographic that shows a high propensity for bullying and harassment.[58]

One solution could be restricting the use of photorealistic avatars to individuals who verify their identity with a face scan or selfie. Then, photorealistic avatars could still be used while avoiding privacy concerns involved with ID verification.[59] Additionally, Meta's Horizon Worlds "bubble" boundary could be instituted across other platforms.

Physically Demanding Experiences

Children can face physically demanding experiences in AR/VR spaces, which include eye strain, fatigue, radiation, and sleep disorders.[60] Adults and children alike can also experience cybersickness, the body's response to the incongruity between the visual information from a VR headset and the body's sense of movement or position, after prolonged use of a headset.

As is the case with prolonged computer monitor, television screen, or smartphone use, eye strain is a common issue when using a device for extended periods of time. VR headsets can potentially affect users' ability to focus, track objects, and perceive depth.[61] Research reveals that young eyes exposed to VR devices absorb higher local radiation doses than is present in adults.[62] Therefore, of all the potential symptoms of cybersickness, the greatest concern in children is the impact on the visual system and its development. However, more research and data are needed to make definitive conclusions, especially because most findings so far have found negligible and only minor long-term impacts.[63]

Children may also be more susceptible to neck strain from the weight of using a headset. Children's neck muscles are less developed than adults', and therefore may be more susceptible to the weight of the device. The average weight of the most popular VR headset is about 1.1 pounds.[64] To put that into perspective, the average child bicycle helmet weighs between 10 and 12 ounces.[65] Headsets such as Oculus and the HTC Vive include safety warnings that their headsets are not designed for users under the age of 13. Oculus warns that improper sizing can lead to physical discomfort and adverse health effects, and that younger children are "in a critical period in visual development."[66]

This area needs further research on long-term impacts, particularly in areas such as visual development, especially for children with cerebral palsy or Down syndrome, who may be more susceptible to already weak eye movement or control.[67]

Developmental Unpreparedness

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. As screens continue to dominate much of a child's daily experience, questions arise as to screens' impact on children's development and cognitive skills, such as memory, attention, and spatial cognition.[68] However, much of the current discourse centers on screens' impact in taking attention and cognition away from children. When these screens become the avenue for immersive experiences, more questions arise as to how attention and cognition are impacted through 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.[69]

Children are also more likely to share personally identifiable information (PII) on the Internet, as a child's comprehension of privacy increases as they get older.[70] This understanding does not always translate to the online world. For example, children can learn to understand real-world privacy concerns, such as safeguarding their home address or the significance of closed doors, but that understanding doesn't always carry over to digital PII, such as voice chats or photos.[71]

Children, whose memory and cognitive skills are still underdeveloped compared with adults, may find it more challenging to process three-dimensional scenes than two-dimensional ones.[72] However, in educational contexts, for example, some studies indicate that AR/VR experiences can improve learning outcomes, motivation, and engagement.[73]

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.[74] The line can become more blurred for children through social realism, or believing a fictional character exists in the real world. When children interact with avatars and fictional characters in AR/VR experiences, children's gravitation toward attachment and building parasocial relationships may be heightened in virtual experiences compared with the characters and individuals in the real world.[75]

For example, the relationships a child has with characters may become more complex if those characters perform harmful actions or harass the child, with the child growing unhealthy behaviors offline because of their attachment to and interactions with the virtual characters.[76] 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 often 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. Therefore, further research should continue to examine how children build these relationships, particularly as it relates to the use of emotion recognition.[77]

Unhealthy Overuse of Technology and Addiction

Compared with adults, children and adolescents are still developing critical thinking and self-regulation skills. Children's ability to understand long-term consequences and deductive reasoning skills are generally not fully developed until around the age of 15 or 16.[78] This lack of development in younger children has implications for activities online that resemble gambling or the supposed addictive nature of platforms and games. Debates around children's use of video games have continued for decades, and these discussions continue and have been extended to include social media platforms as well. While some argue AR/VR gaming is more addictive than other types of video games, concerns over children's ease in becoming addicted to any technology are unfounded in research.[79] However, gaming design features that resemble gambling, such as loot boxes, tokens, and virtual rewards, prey on children's inability to understand that they are being manipulated to spend money or more time playing a game.

A loot box is an in-game container with one or more random objects players must spend real or in-game currency on that makes the player more powerful or competitive in the game. Because the player obtains the reward at random, players are incentivized to buy more of the reward to have a better chance of achieving the better prizes. The Federal Trade Commission (FTC) has identified loot boxes as a national and international concern, as they can encourage gambling-like behaviors and use tactics to encourage addictive spending.[80] Some games allow users to unlock loot boxes by completing in-game tasks or logging into the games within regular time periods. In addition, many video games have evolved from one-time purchases to service platforms wherein the games are free but rely on in-app purchases to create revenue. Because of children's lack of understanding of long-term consequences and their desire for play, they might not understand that their purchases within the games occur in the real world too.

Developers need to balance making a game compelling and entertaining to play while looking out for children's best interests. The video game industry, either voluntarily or due to proposed regulatory mandates, has introduced various measures to minimize the negative effects of gambling-like mechanics such as loot boxes. These measures include setting spending limits for underage accounts to $0 by default, disclosing every item included in a loot box's pool alongside their drop rate (how likely a player is to get the best item), and imposing hourly and daily limits on purchases of loot boxes by an individual user.[81] Given the expectation that AR/VR experiences will support and carry betting apps, it is important to understand that children may interact with these platforms and, as a result, may experience gambling-like situations and behaviors. Furthermore, games that require a certain amount of time playing them in order to unlock rewards may incentivize unhealthy gaming behaviors, such as deprioritizing sleep to continue playing.[82]

However, time-online policies are difficult for policymakers to enforce. China, for example, instituted a three-hour-per-week limit for children playing video games. While 77 percent of children reduced their gaming time under this policy, 29 percent of children also reported using their parents' accounts as a workaround to the time limit.[83] Some platforms have taken voluntary steps to tackle any potential harms, with measures such as allowing users to limit their screen time and see screen-time reports, or notifying them to take a break whenever they have spent a certain amount of time on an app.

Rather than implementing overly restrictive policies that hinder user experience and halt innovation in the space, many technology companies instead adopt user and parental control systems such as screen- time controls and prompts to take breaks after using the apps for extended periods of time.[84]

Lastly, in-game advertising scenarios are another methodology platforms use to keep children online and part of the gaming experience that children may not understand can be manipulative. The FTC has found that children find it difficult to distinguish between advertising and other forms of content, which can prompt them to make accidental purchases or unintentionally share private information.[85] This is made worse when the advertisements use children's parasocial relationships with fictional characters or kidfluencers to persuade them. Even ad disclosures are not effective on children because adults can typically understand when content is presented or labeled as an advertisement, but only 10 percent of children understand the meaning of "paid advertisement."[86] However, targeted ads will likely encompass a vast portion of the digital economy in the metaverse and are already an integral part of the mostly free Internet economy.[87] To best address this issue, a federal privacy law should give consumers of all ages more control over their personal data and require greater transparency in online advertising to address deceptive practices.[88]

RECOMMENDATIONS

Children's online safety is a global, trending policy issue. An effective approach to children's online safety in AR/VR and the metaverse, as in 2D online experiences, needs to strike a balance between protecting kids, protecting user privacy, and protecting free speech, as well as striking a balance between giving responsibility to the government, online services, and parents.[89] Such an approach should include the following:

1. Congress should pass comprehensive federal privacy legislation that addresses actual privacy harms and preempts state laws, creating a single set of protections for all Americans, including children.[90]
2. The Kids Online Safety Act (KOSA) and the Children and Teens' Online Privacy Protection Act (COPPA 2.0) (collectively "KOPSA"), which passed in the U.S. Senate on July 30, 2024, includes in its definition of covered online platforms language regarding protections for children in the "virtual reality environment."[91] If KOPSA passes in the U.S. House and becomes law, AR/VR platforms may be forced to ramp up enforcement in the same manner as traditional social media platforms.[92] In so doing, by giving the FTC authority to deem content on these platforms as harmful, the FTC may over-censor content on AR/VR platforms or platforms themselves may censor content to avoid liability, which could include content pertinent to children's education, entertainment, and identity.[93]
3. Congress should pass legislation requiring device operating systems to create an opt-in "trustworthy child flag" for user accounts, available when first setting up a device and later in a device's settings, that signals to apps and websites that a user is underage and requiring apps and websites that serve age-restricted content to check for this signal for their users and block underage users from such content.
4. Congress should pass legislation establishing 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.
5. Congress should pass federal legislation similar to the Coogan Act and Illinois' child influencer legislation that protects child performers in traditional and digital media by requiring parents to set aside a portion of a child's earnings in a trust that the child can access upon reaching adulthood. Then, kidfluencers' parents or managers are legally responsible for failing to set aside a portion of kidfluencers' incomes, mirroring protections afforded to other child entertainers.[94]
6. Congress 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.
7. Congress should provide funding for research on the long-term physical health impacts and developmental implications of AR/VR, especially as it relates to the development of

children’s cognitive skills, relationship building with virtual characters, and vision development.

8. NIST should develop guidelines for integrating biometric identity verification methods securely into immersive platforms and integrate this in its Digital Identity Guidelines.[95] These guidelines provide technical requirements for digital identity management, especially as it relates to authentication and usability of digital identity solutions.[96] Adding additional guidance for biometric identity verification for AR/VR, such as fingerprints, voiceprints, iris scans, and facial recognition, should ensure better privacy and security protections for users.[97]

CONCLUSION

As the drivers of the metaverse, children play a crucial role in the market adoption of immersive technologies. Ensuring innovation can flourish in this nascent field while also creating a safe environment for all users of AR/VR technology will be a complex challenge. Parents, corporations, and regulators all have roles to play by balancing privacy and safety concerns while creating engaging and innovative immersive experiences.

About the Author

Alex Ambrose is a policy analyst at ITIF focusing on augmented and virtual reality, as well as children’s online safety and privacy. She previously worked at ITIF as a communications manager. She holds a B.S. in public relations from Syracuse University and an M.P.A. in public policy analysis from Indiana University.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent 501(c)(3) nonprofit, nonpartisan research and educational institute that has been recognized repeatedly as the world’s leading think tank for science and technology policy. Its mission is to formulate, evaluate, and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. For more information, visit itif.org/about.

ENDNOTES

[1] Vivek H. Murthy, "Surgeon General: Why I'm Calling for a Warning Label on Social Media Platforms," *The New York Times*, June 17, 2024, https://www.nytimes.com/2024/06/17/opinion/social-media-health-warning.html; Alex Ambrose and Daniel Castro, "The Surgeon General's Misleading Claims About Social Media's Risk to Children Should Come With Its Own Warning Label" (ITIF, June 25, 2024), https://itif.org/publications/2024/06/25/surgeon-generals-misleading-claims-should-come-with-own-warning-label/.

[2] 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/; Juan Londoño, "User Safety in AR/VR: Protecting Teens" (ITIF, February 5, 2024), https://itif.org/publications/2024/02/05/user-safety-in-ar-vr-protecting-teens/.

[3] Kenneth R. Ginsburg, "The Importance of Play in Promoting Health Child Development and Maintaining Strong Parent-Child Bonds," American Academy of Pediatrics, January 1, 2007, https://publications.aap.org/pediatrics/article/119/1/182/70699/The-Importance-of-Play-in-Promoting-Healthy-Child.

[4] Search for #ARVRsafety on itif.org: https://itif.org/search/?skeyword=%23ARVRsafety.

[5] Ash Johnson, "How to Improve the American Privacy Rights Act" (ITIF, June 6, 2024), https://itif.org/publications/2024/06/06/how-to-improve-the-american-privacy-rights-act/.

[6] Alex Ambrose, "Comments Before the 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/.

[7] 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.

[8] Ibid.

[9] "The importance of pretend play in child development," *Bright Horizons*, May 28, 2024, https://www.brighthorizons.com/resources/Article/Importance-of-Pretend-Play-in-Child-Development.

[10] "2023 Essential Facts About the U.S. Video Game Industry," *Entertainment Software Association*, accessed on June 7, 2024, https://www.theesa.com/resources/essential-facts-about-the-us-video-game-industry/2023-2/.

[11] Ibid.

[12] Juan Londoño, "User Safety in AR/VR: Protecting Teens."

[13] Seth G. Macy, "Looking Back at the Virtual Boy, Ninetendo's Most Famous Failure," IGN, July 21, 2023, https://www.ign.com/articles/looking-back-at-the-virtual-boy-nintendos-most-famous-failure; Juli Clover, "Apple Has Sold Approximately 200,000 Vision Pro Headsets," MacRumors, January 29, 2024, https://www.macrumors.com/2024/01/29/apple-vision-pro-headset-sales/.

[14] Daniel Kardefelt Winther, "Responsible Innovation in Technology for Children," *UNICEF*, April 2024, https://www.unicef.org/innocenti/reports/responsible-innovation-technology-children.

[15] "Children's Views on Gaming," *Boston Children's Digital Wellness Lab*, September 2023, https://digitalwellnesslab.org/research-briefs/childrens-views-on-gaming/.

[16] Ibid.

[17] Ibid.

[18] Jana Arbanas et al., “For women playing video games, it’s (still) a man’s world,” *Deloitte*, March 20, 2024, https://www2.deloitte.com/us/en/insights/industry/technology/digital-media-trends-consumption-habits-survey/2024/how-can-gaming-industry-get-more-female-gamers.html.

[19] Jacqueline Howard, “What’s the average age when kids get a social media account?” *CNN*, June 22, 2018, https://www.cnn.com/2018/06/22/health/social-media-for-kids-parent-curve/index.html.

[20] Alex Ambrose, “Kidfluencers Recast Spotlight On Children’s Rights in Digital Entertainment” (ITIF, September 5, 2023), https://itif.org/publications/2023/09/05/kidfluencers-recast-spotlight-on-children-s-rights-in-digital-entertainment/.

[21] “Gen Zers Still Really Want to Be Influencers,” *Morning Consult*, October 4, 2023, https://pro.morningconsult.com/analysis/gen-z-interest-influencer-marketing.

[22] Stacey Steinberg, “Ethical AI? Children’s Rights and Autonomy in Digital Spaces*,” London School of Economics*, April 28, 2021, https://blogs.lse.ac.uk/parenting4digitalfuture/2021/04/28/children-and-ai/.

[23] Ibid.

[24] Londoño, “User Safety in AR/VR: Protecting Teens.”

[25] “Online Safety Across the Generations,” *Family Online Safety Institute*, 2018, https://fosi-assets.s3.amazonaws.com/media/documents/2018Report_FR_d6_web.pdf; Londoño, “User Safety in AR/VR: Protecting Teens.”

[26] Johnson, “How to Address Children’s Online Safety in the United States”; Londoño, “User Safety in AR/VR: Protecting Teens.”

[27] 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/.

[28] 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/.

[29] 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.

[30] Dick, “The Promise of Immersive Learning: Augmented and Virtual Reality’s Potential in Education.”

[31] Ibid.

[32] Shailaja Neelakantan, “Schools Face Barriers to VR Adoption in the Classroom,” *EdTech Magazine*, December 2, 2019, https://edtechmagazine.com/k12/article/2019/12/schools-face-barriers-vr-adoption-classroom; Brandon Paykamian, “What Could AR/VR Do for Social and Emotional Learning?” *Government Technology*, March 1, 2024, https://www.govtech.com/education/k-12/what-could-ar-vr-do-for-social-and-emotional-learning.

[33] Alyson Klein, “5 Big Technology Challenges Teachers and Administrators Will Face This School Year,” *Education Week*, August 26, 2022, https://www.edweek.org/technology/5-big-technology-challenges-teachers-and-administrators-will-face-this-school-year/2022/08.

[34] Londoño, “User Safety in AR/VR: Protecting Teens”; 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/.

[35] Londoño, “User Safety in AR/VR: Protecting Adults.”

[36] Scott Stein, “Please, Don’t Walk Around Outside Wearing an Apple Vision Pro,” *CNET*, February 13, 2024, https://www.cnet.com/tech/computing/please-dont-walk-around-wearing-vision-pro/.

37. Johnson, “How to Address Children’s Online Safety in the United States.”
38. Chloe Setter et al., “Global Threat Assessment 2021,” *WeProtect Global Alliance*, 2021, accessed on May 22, 2024, https://www.weprotect.org/global-threat-assessment-21/#report.
39. Johnson, “How to Address Children’s Online Safety in the United States.”
40. Ash Johnson, “How Congress Can Foster a Digital Single Market in America” (ITIF, February 20, 2024), https://itif.org/publications/2024/02/20/how-congress-can-foster-a-digital-single-market-in-america/.
41. “US State age verification laws for adult content,” *Age Verification Providers Association*, June 2024, https://avpassociation.com/4271-2/.
42. Johnson, “How to Address Children’s Online Safety in the United States.”
43. Johnson, “How to Improve the American Privacy Rights Act.”
44. Johnson, “How to Address Children’s Online Safety in the United States.”
45. “What is grooming?” *National Society for the Prevention of Cruelty to Children*, accessed on May 22, 2024, https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/.
46. “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.
47. Reed and Joseff, “Kids and the Metaverse.”
48. Sameer Hindjua, “Child Grooming and the Metaverse—Issues and Solutions,” *Cyberbullying Research Center*, accessed on May 22, 2024, https://cyberbullying.org/child-grooming-metaverse.
49. “Protection of children from the harmful impacts of pornography,” *UNICEF*, accessed on June 10, 2024, https://www.unicef.org/harmful-content-online.
50. “Age of First Exposure to Pornography Shapes Men’s Attitudes Toward Women,” *American Psychological Association*, 2017, https://www.apa.org/news/press/releases/2017/08/pornography-exposure; “Teens and Pornography,” *Common Sense Media*, January 10, 2023, https://www.commonsensemedia.org/research/teens-and-pornography.
51. Johnson, “How Congress Can Foster a Digital Single Market in America.”
52. Londoño, “User Safety in AR/VR: Protecting Adults.”
53. Londoño, “User Safety in AR/VR: Protecting Teens.”
54. Reed and Joseff, “Kids and the Metaverse.”
55. Londoño, “User Safety in AR/VR: Protecting Teens.”
56. Naomi Nix, “Meta doesn’t want to policy the metaverse. Kids are paying the price,” *The Washington Post*, March 8, 2023, https://www.washingtonpost.com/technology/2023/03/08/metaverse-horizon-worlds-kids-harassment/.
57. Naomi Nix, “Attacks in the metaverse are booming. Police are starting to pay attention,” *The Washington Post*, February 6, 2024, https://www.washingtonpost.com/technology/2024/02/04/metaverse-sexual-assault-prosecution/.
58. Ibid.
59. Londoño, “User Safety in AR/VR: Protecting Adults.”
60. 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/.

61. Maria Diaz, “Are VR headsets safe for kids and teenagers? Here’s what the experts say,” *ZDNet*, accessed on May 9, 2024, https://www.zdnet.com/article/are-vr-headsets-safe-for-kids-and-teenagers-heres-what-the-experts-say/.

62. Claudio Fernández et al., “Absorption of wireless radiation in the child versus adult brain and eye from cell phone conversation or virtual reality,” Environmental Research, vol. 167, accessed on May, 8, 2024, https://www.sciencedirect.com/science/article/abs/pii/S0013935118302561.

63. Kaimara, Oikonomou, and Deliyannis, “Could virtual reality applications post real risks to children and adolescents? A systematic review of ethical issues and concerns.”

64. Marla Broadway, “Meta Quest 3 weight—how heavy is it?” *PC Guide*, October 3, 2023, https://www.pcguide.com/vr/meta-quest-3-weight/.

65. “Our Ideas on the Ideal Helmet,” *Bicycle Helmet Safety Institute*, accessed on June 24, 2024, https://www.helmets.org/ideal.htm.

66. “Health and Safety Before Using the Headset,” *Meta*, https://securecdn.oculus.com/sr/oculusgo-warning-english.

67. Kaimara, Oikonomou, and Deliyannis, “Could virtual reality applications post real risks to children and adolescents? A systematic review of ethical issues and concerns.”

68. Ibid.

69. Ibid.

70. 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.

71. 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/.

72. Kaimara, Oikonomou, and Deliyannis, “Could virtual reality applications post real risks to children and adolescents? A systematic review of ethical issues and concerns.”

73. 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/.

74. Angela Haupt, “In Defense of Parasocial Relationships,” *Time*, July 23, 2023, https://time.com/6294226/parasocial-relationships-benefits/.

75. 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.

76. 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#.

77. 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.

78. Kara Rogers, “Formal operational stage,” *Encyclopedia Britannica*, July 12, 2023, https://www.britannica.com/science/formal-operational-stage.

79. Kaimara, Oikonomou, and Deliyannis, “Could virtual reality applications post real risks to children and adolescents? A systematic review of ethical issues and concerns.”

[80] Lesley Fair, “Loot Boxes: What’s in play?” *Federal Trade Commission*, August 14, 2020, https://www.ftc.gov/business-guidance/blog/2020/08/loot-boxes-whats-play.

[81] Londoño, “User Safety in AR/VR: Protecting Teens”; Patricia E. Vance, “What Parents Need to Know About Loot Boxes (and Other In-Game Purchases),”*Entertainment Software Rating Board*, July 12, 2023, https://www.esrb.org/blog/what-parents-need-to-know-about-loot-boxes-and-other-in-game-purchases/.

[82] Peter Grinspoon, “The health effects of too much gaming,” *Harvard Health Publishing*, December 22, 2020, https://www.health.harvard.edu/blog/the-health-effects-of-too-much-gaming-2020122221645.

[83] Zeyi Yang, “China is escalating its war on kids’ screen time,” *MIT Technology Review*, accessed on May 3, 2024, https://www.technologyreview.com/2023/08/09/1077567/china-children-screen-time-regulation.

[84] Londoño, “User Safety in AR/VR: Protecting Adults.”

[85] Alexander Lee, “Why regulators at the FTC and beyond are turning an eye to child safety in gaming in 2023,” *Digiday*, September 20, 2023, https://digiday.com/marketing/why-regulators-at-the-ftc-and-beyond-are-turning-an-eye-to-child-safety-in-gaming-in-2023/.

[86] Alex LaCasse, “FTC event on digital advertising to children looks at brand-influencer relationships,” *IAPP*, October 24, 2022, https://iapp.org/news/a/ftc-panels-on-digital-advertising-to-children-focuses-on-disclosures-of-brand-influencer-relationships.

[87] Ash Johnson, “Banning Targeted Ads Would Sink the Internet Economy” (ITIF, January 20, 2022), https://itif.org/publications/2022/01/20/banning-targeted-ads-would-sink-internet-economy/.

[88] Ash Johnson, “Banning Ads for Kids: An Old, Bad Idea” (ITIF, June 25, 2024), https://itif.org/publications/2024/06/25/banning-ads-for-kids-an-old-bad-idea/.

[89] Johnson, “How to Address Children’s Online Safety in the United States.”

[90] Johnson, “How to Improve the American Privacy Rights Act.”

[91] “S.Amdt.3021 to S.2073 - 118th Congress (2023-2024),” July 30, 2024, https://www.congress.gov/amendment/118th-congress/senate-amendment/3021/text.

[92] Derek Robertson, “The long road to child safety in the metaverse,” *POLITICO*, July 31, 2024, https://www.politico.com/newsletters/digital-future-daily/2024/07/31/the-long-road-to-child-safety-in-the-metaverse-00172137.

[93] Ash Johnson, “Senate Rushes to Pass Flawed Children’s Privacy and Online Safety Bills, Says ITIF” (ITIF, July 30, 2024), https://itif.org/publications/2024/07/30/senate-rushes-to-pass-flawed-childrens-privacy-online-safety-bills/.

[94] Ambrose, “Kidfluencers Recast Spotlight on Children’s Rights in Digital Entertainment.”

[95] Alex Ambrose, “Comments Before the 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/.

[96] “Digital Identity Guidelines,” *NIST*, accessed on July 31, 2024, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

[97] Ambrose, “Comments Before the NIST Regarding Preliminary Research on Cybersecurity and Privacy Standards for Immersive Technologies.”