ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

User Safety in AR/VR: Protecting Adults

JUAN LONDOÑO | JANUARY 2023

Policymakers should empower metaverse platforms to develop innovative tools and solutions to address safety issues and ensure AR/VR products and services don't harm users. Overly prescriptive regulation risks stifling the progress of those innovations.

KEY TAKEAWAYS

- Addressing user safety in AR/VR will require action from various stakeholders. Before enacting regulations, policymakers should recognize platforms' ongoing efforts to create safe environments and develop tools for users to protect themselves.

- Personalized threats can often be tackled by providing users with tools such as muting, blocking, or reporting. Meanwhile, platforms can address systemic issues through content moderation, design tools, and industry best practices.

- As with most novel technologies, creating a safe environment in AR/VR will require experimentation with different tools and approaches. Policymakers should be wary of regulations that could stifle the industry's ability to experiment freely.

- Policymakers can most effectively advance user safety in AR/VR by taking steps such as codifying digital crimes, training law enforcement, and supporting necessary research.

CONTENTS

INTRODUCTION

Over the past decade, augmented reality (AR) and virtual reality (VR)—immersive technologies that enable users to experience digitally rendered content in both physical and virtual space—have seen continuous growth and maturation, evolving from niche products for special applications into general-purpose technologies with significant potential to transform the way consumers shop, businesses manufacture goods, and people socialize with each other. Recently, there have been multiple initiatives from leading tech companies to launch AR/VR products, indicating their commitment to the technology and bringing the technology into the mainstream. The rebranding of Facebook, one of the biggest tech companies globally, as Meta provides the highest-profile example of one of the sector's visions for how AR/VR may significantly shape the future of the Internet.

As AR/VR technologies enter the mainstream, one priority is addressing user safety: ensuring AR/VR products and services do not cause injury, harm, or loss to users. Due to the broad impact AR/VR technologies can have on multiple aspects of a user's life—the technology can provoke physical and psychological sensations—user safety covers a wider range of issues beyond physical threats, including psychological and financial well-being.[1]

While many of the user safety issues present in AR/VR are similar to its technological predecessors, such as smartphones and videogames, the level of immersion AR/VR aims to achieve can increase the magnitude or complexity of these risks. For example, the installation of spyware in an AR device intended for all-day use and equipped with a front-facing camera could potentially reveal a more significant amount of sensitive information in comparison with a compromised smartphone. Or the heightened sensory load of a VR headset can make the physical effects, such as motion sickness, more acute.

While many of the user safety issues present in AR/VR are similar to its technological predecessors, the level of immersion AR/VR aims to achieve can increase the magnitude or complexity of these risks.

Addressing user safety in AR/VR will require various stakeholders—from hardware manufacturers and online platforms to users—to develop and use a wide range of tools. For example, personalized threats—such as a particular case of harassment—may best be addressed by creating tools to empower individual users to mute or block others. Meanwhile, threats to communities, such as hate speech, might better be addressed by creating content moderation tools for platform operators. Other threats may be addressed by some combination of both, such as design changes to AR/VR platforms or reporting tools that allow users to notify platform operators of violations of community guidelines. Thoughtful policy will also play a role, but before enacting regulations for AR/VR technologies, policymakers should consider the ongoing effort by AR/VR developers to create user safety tools and ensure they do not erode the capacity of these tools to provide a safe user experience.

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 below 13). These divisions correspond to differences in how regulations treat each of these demographics and the unique risks they face.

This report concludes the following:

- Policymakers should consider the potential negative impact of proposed laws and regulation on social media, biometrics, and content moderation on AR/VR.
- Congress should enact federal legislation across all 50 states that criminalizes such harmful actions as cyberbullying, distributing revenge porn, and swatting.
- The Department of Justice should create guidelines for local and state police departments that raise awareness of these cybercrimes and provide tools for police officers to respond accordingly.
- The Department of Labor should fund research grants on eye strain and motion sickness in AR/VR to address worker safety issues.
- The National Highway Traffic Safety Administration (NHTSA) should update its distracted driving guidance to explicitly address issues specific to AR heads-up displays (HUDs) in vehicles.
- The National Institutes of Health should support research on potential psychological harms derived from the continuous use of AR/VR devices.

AN OVERVIEW OF AR/VR TECHNOLOGY

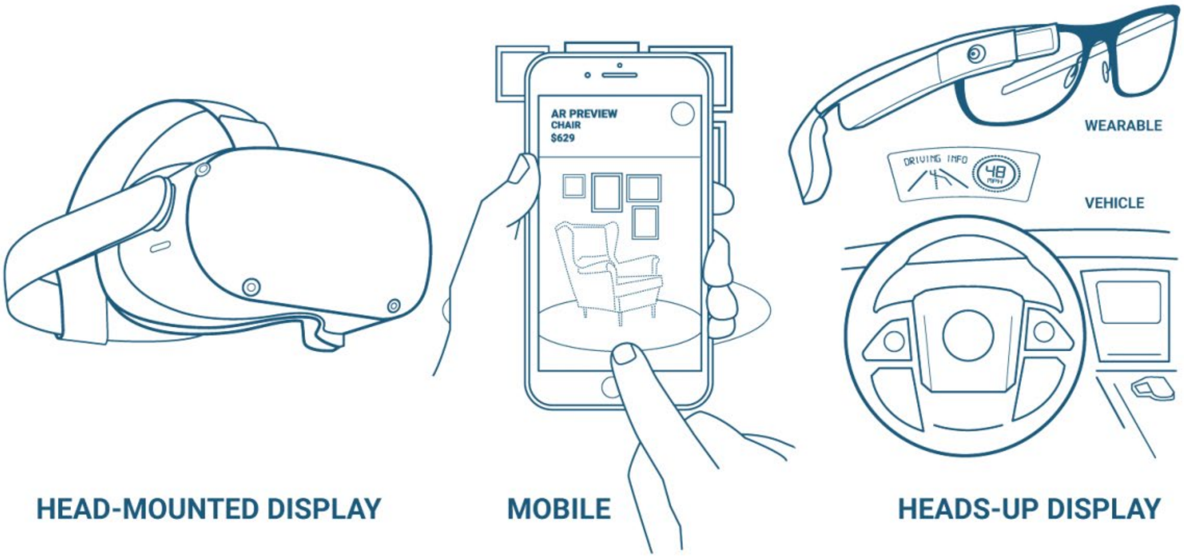
Immersive technologies allow users to see and interact with digitally rendered content.[2] These technologies are divided into three categories depending on their targeted level of user immersion and their reliance on digital and physical imagery: VR, AR, and mixed reality (MR). VR technology focuses mainly, if not exclusively, on digital content and images, usually restricting users' visuals to the images displayed on their screens. On the other side, AR technology relies more on the physical world and aims to create a "digital layer" of imagery on top of images in the real world. MR technologies, as their name indicates, opt for a mixed approach wherein there is a prominent use of digital imagery but physical images are still used. MR is also a commonly used concept to describe devices that can easily switch from AR to VR functionalities.

AR/VR devices can vary depending on their desired level of immersion, portability, and intended use. VR hardware, for example, tends to focus exclusively on head-mounted displays (HMDs) to block external images and provide a more immersive experience. Meanwhile, AR hardware tends to use HUDs in vehicles and wearables such as smart glasses, allowing users to see the digital images without disrupting their vision of the physical world. AR technology can also be more commonly seen in modern smartphones, which have gained the processing capability to render digital images in real time by using their cameras.

The introduction of Google Glass, Google's AR glasses, at the start of the past decade raised multiple concerns ranging from road safety to bystander privacy. While Google Glass did not find the commercial success the company had envisioned at its launch, it provided a valuable blueprint for the sector, highlighting the main priorities these companies ought to look into to build a safe AR/VR product and environment.[3]

User safety will look different for a technology depending on where it is in its development cycle. In earlier stages, the technology is a niche product with limited use cases, such as for enthusiasts and specific business applications. Users tend to be tech savvy and use the technology in more controlled environments, thereby limiting accidents. As technologies mature and adoption increases, they are used in less-controlled environments and by less-tech-savvy users, which can expose new risks and practices that were probably overlooked in earlier stages. Currently, AR/VR technologies are in the "family computer" stage in which households usually own one device that's shared by all members.

Figure 1: Types of immersive technologies



Unlike smartphones or computers, AR/VR is generally regarded as a luxury item, as consumers have not yet integrated the technology into day-to-day routines. Thus, users are aware that they share these devices, altering their behavior and the information they are willing to share while using them. Having a shared device for a household usually means behavior tends to be restrained by the fact that other members of the household might be aware of its use or even be physically observing them while using the device. It might also prevent users from sharing certain personal information they would otherwise share if the device were personal. Today's threats to users' safety might look different from the ones of the future, when the user base has expanded to the point where individuals commonly own a personal AR/VR device.

ARE AR/VR'S RISKS DIFFERENT FROM THOSE PRESENT IN CURRENT TECHNOLOGIES?

The evolution of AR/VR technologies shows how certain tech products, such as smartphones and social media, have heavily influenced AR/VR's development. In many cases, AR/VR tech hopes to leverage the proven success of these technologies by integrating most of their core functionality. But it may inherit similar user safety challenges, as well as new ones or ones that have yet to be resolved in existing technologies. This section reviews some of those shared threats and highlights AR/VR's unique threats.

Similarities

There are a number of similarities between wearables and smartphones and multi-user immersive experiences and 2D social media.

AR/VR Wearables, Digital Cameras, and Smartphones

Always-on AR/VR wearables designed for general users share many of the same challenges smartphones faced in the past or continue to face up to this day. One of the main shared concerns between these devices is related to the capabilities of both devices to capture pictures and video in a relatively easy way. The concern over the ease of recording bystanders is a long-standing privacy concern that goes back to the first introduction of the camera, which created concerns regarding third parties.[4] With AR/VR, there are concerns that some wearables will allow people to photograph or record bystanders in public spaces without their consent.[5] Some of these concerns are rooted in a lack of social norms and social cues that notify others that someone is using the device to record, due to the novelty of the devices. Additionally, most of these wearables expect to be heavily reliant on online social media.[6] This reliance will likely mean AR/VR wearables will share similar privacy concerns to those associated with the use of online social media on smartphones, such as location and activity tracking.

Another shared concern is that using these devices while driving, biking, or walking may present safety risks by distracting users.[7] While smartphones can use GPS to help pedestrians and drivers navigate to a destination, they can also distract users. For example, features such as music streaming and social media notifications can distract individuals or impair their response, potentially causing accidents on the road.[8]

Multi-user Immersive Experiences and 2D Social Media

Multi-user immersive experiences (MUIE) are potentially the next evolutionary step in social interaction, broadening the capacities of current 2D social media by providing a more immersive experience, with a more robust entertainment offering. MUIEs will allow users to use nonverbal communication, attend and actively participate in live events, and create a fully digital identity, usually represented in their avatar. Nonetheless, the central dynamic of MUEIs is similar to what is seen in 2D social media: Users of a particular platform interact with each other, share content for a specific audience, and create a bond over this online interaction.

The similarity between MUIEs and social media is reflected in the concerns regarding the content accessible to users of the platform: Content shared by a user can lead to the spread of misinformation during political events, which can spark widespread panic among the population during uncertain times, such as a nationwide protest.[9] Misinformation can create public health crises, such as the cases where a viral social media challenge incentivized users to eat toxic materials such as detergent.[10] A user can publish content that leads to the harassment of another user or calls for real-world violence among said user or a group of people.

Similarly, the MUIE platform's role in collecting and protecting users' data will make them responsible for setting appropriate privacy policies and data security protocols. The messages and interactions happening in these worlds will have to go through the platform's servers, and just like with 2D platforms, the platform's approach to data privacy and security will have an impact on how MUIE platforms can address user safety.

Like on 2D social media, MUIE users may create a new digital identity that differs from their physical-world counterpart, allowing them to lower their inhibitions and act in ways they would not in the physical world. And while this freedom presents an opportunity for increased individual expression and creativity, it might give rise to antisocial behavior.[11] The always-online nature of the metaverse could magnify the impact of this behavior, as current consumer-focused AR/VR products have placed heavy emphasis on social AR/VR as their core feature. If digital identities become a more prominent aspect of an individual's life, as social AR/VR aims to achieve, these negative experiences could be more impactful on a user's psyche.

Internet of Things and Always-On Devices

The mass adoption of Internet of Things (IoT) devices has demonstrated that a lot of the devices used for day-to-day activities—such as lights, locks, and thermostats—could benefit from adding "smart" functionalities. By adding computational resources and Internet connectivity, these devices are better equipped to respond to the user's needs and specific contexts, receive ongoing maintenance and firmware updates, and allow for a deeper integration with other Internet-enabled devices. But the rise of IoT devices has also highlighted how always-online products can bring a wide range of threats—from physical to mental to financial—compared with their "analog" versions.

The adoption of IoT devices sheds light on the importance of cybersecurity as a priority in the design process. The smart functionality of these devices and their always-online nature makes them susceptible to hacking and malware that could put their users at risk. For example, a hacked device could potentially compromise a user's location or cause a smart appliance to overheat and catch fire.[12] The same risks exist with AR/VR devices. Most of these devices will use multiple cameras and sensors in order to function, which could potentially reveal sensitive information—such as location data—if attackers compromise them. If the device is intended for continuous use, such as a wearable, it could reveal even more information about a user's routine, such as their day-to-day conversations or even passwords.

Differences

Despite the numerous similarities between AR/VR technology and previous technologies, user safety in AR/VR introduces more complex challenges due to the immersive nature of the technology, which generally requires an increased amount of data collection, user attention, use of cameras, and sensory load.[13] There are additional concerns regarding the use of screens that are usually placed a few inches away from the user's eyes, particularly for long periods of time. In the case of VR, some of the safety concerns are linked to the use of the hardware (which can often blind a user from their surroundings) and the speed at which the images are shown in a headset (which can induce motion sickness).

Because AR/VR is an emerging technology, there is little scientific research that can accurately assess the psychological risks associated with its use. The uncertainty caused by the lack of a scientific consensus makes it possible to both underestimate and overestimate the actual dangers associated with the use of the technology. The hypothetical threats discussed today may be very different from what the real threats will be in the future, as the threats that are theoretically feasible might fail to materialize in practice.

CURRENT THREATS TO USER SAFETY IN AR/VR TECHNOLOGY

AR/VR will provide users with a more intense experience in comparison with those confined to 2D screens. Its immersive nature, alongside the option of using haptic accessories, generates a higher sense of embodiment, where users not only consume content, but also feel present in it. While this immersiveness will allow for new beneficial uses of technology, it might bring new threats to user safety that were not present before, spanning physical, psychological, financial, or even societal harms.

Table 1: Summary of known threats and potential responses

Type of Threat	Where It Occurs	Potential Solutions
Distracted driving/biking/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
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 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 live streaming ▪ Privacy and data stewardship standard setting ▪ Federal privacy legislation
Leading users to dangerous/off-limits locations	Augmented reality	▪ Geofencing ▪ Robust reporting system ▪ Conscious product design, which is mindful of hazardous areas
Incitation of violence/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 in MUIEs	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

Type of Threat	Where It Occurs	Potential Solutions
		▪ 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
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 (ESRB) 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 password-less technology such as Zero-Trust Authentication
Impersonation and reputational damage	Multi-user immersive experiences	▪ Impersonation report systems ▪ Locking photorealistic avatar function for nonverified users

Physical Harms

One of the biggest draws for AR/VR technology is the way the users consume content. Immersive technologies allow users to be actively present in the content by using their bodies. But by introducing physical activity into content consumption, AR/VR use introduces a new range of risks in comparison with 2D devices. These risks range from eye strain and motion sickness to crashing into furniture and distracted driving, for example.

Distracted Driving, Biking, and Walking

One of the most noticeable safety concerns with AR technology is the possibility of distracting users that drive or walk while using their devices. AR products, such as the Nreal Light or Meta's upcoming AR glasses (codenamed as Project Aria), could come with practical tools that facilitate commuting, such as precise GPS, allowing users to get to their destination without taking their eyes off the road or sidewalk.[14] But they can also prove distracting to users, as notifications from applications could cause users to lose focus on their environment, potentially resulting in an accident or mishap.

Different bills and laws are addressing these types of concerns. For example, 48 U.S. states have laws that ban texting while driving.[15] Some cities, such as Honolulu, fine pedestrians who stare at a screen while walking in a crosswalk.[16] Meanwhile, in some states, such as West Virginia, legislators have pushed legislation specific to AR/VR products, such as a bill that intended to ban the use of Google Glass while driving. [17]

This issue does not affect all AR products equally. HUD devices, particularly those in vehicles, tend to both be less distracting for users and exclusively support driving-related applications. As manufacturers design these products solely for vehicles, road safety is embedded in the product's design. Currently, AR-powered HUDs tend to be offered mostly in luxury car brands, but a number of mainstream brands also offer it as a premium feature, and market analysts expect HUDs to become more affordable and common as early as 2024.[18] As the technology evolves and matures, it is likely that new problems—and solutions—will arise.

Other products with a broader array of applications, such as wearables and smartphones, may prove to be more problematic, as their wider toolbox may inadvertently make them more prone to distract users due to the presence of distracting applications—such as social media—or because they might require users to look away from the road to use them, as is the case with smartphones. Nonetheless, there have been software-side measures in recent years that tackle this issue. An example of this is Apple's and Google's introduction of different "focus" modes on their mobile operating systems that allow users to enable "driving" mode, which users can customize to limit notification pop-ups and sounds, thereby reducing distractions while on the road.[19] Another example is the moving vehicle pop-up feature in the Waze navigation app, which aims to prevent users from imputing text in the app if it detects that they are in a moving vehicle unless they confirm they are in the passenger seat.

Motion Sickness

Since the popularization of VR technology, there has been an increasing number of reports and supporting research finding that the use of VR HMDs has caused motion sickness among users, despite their being stationary. This sickness is usually caused by the discrepancy between the moving imagery in virtual environments and the lack of actual movement, which can confuse the brain, as the eyes perceive movement but the systems providing equilibrium do not perceive any movement. This experience can cause discomfort to users both during and after the use of VR HMDs, leaving them sick for extended periods of time, ranging from hours to multiple days after use.[20]

Motion sickness is a rather individualized issue, as the frequency and magnitude of the sickness vary by individual. Thus, app developers have mainly addressed this issue by introducing a wide range of modifiers that have proven effective in combating motion sickness. One of the most common measures is limiting users' field of view, creating a "tunnel vision" effect, which helps ease motion sickness, particularly when users move in virtual worlds. Another common measure is allowing users to customize various movement settings, such as teleporting—where a user's avatar moves by phasing in and out of its previous location instead of a smooth, uninterrupted movement—camera rotation speed, or rotation angle. Technological limitations have also been identified as a sickness-inducing factor, such as screen lag or flicker. It is expected that as computational power increases and manufacturing costs go down, headsets will be equipped with better screens and processors that will ameliorate this issue.[21]

Eye Strain

Most VR HMDs are designed such that users will be staring into screens that are mere inches away from their eyes. Concerns over the potential for eye strain has prompted research regarding the potential impact of the continuous use of screens at that distance.[22] While not discussing VR specifically, the Mayo Clinic has noted, "Extended use of computers and other digital devices is one of the most common causes of eyestrain."[23]

The exact impact of VR use on users' eyes is still under-researched. Nonetheless, both users and developers have access to different tools that could combat extended screen time. From the developer side, tools such as screen time reports and pop-ups can prompt users to take a break from using the devices. Users also can take voluntary breaks, although doing so does require some level of technological literacy from users so they are aware of the problem in the first place.

Obscured or Limited Field of View

The use of AR/VR HMDs or HUDs can, in some cases, obscure or limit the user's field of view, restraining their capacity to assess their environment. The level of immersion that can happen while using AR/VR tech, particularly VR, can put users at risk of hurting themselves by moving into objects or dangerous areas, such as surrounding furniture or appliances.[24] Most VR HMDs have attempted to tackle this problem by establishing a virtual boundary or alert system that notifies users when they go beyond a previously determined area.

Nevertheless, there are instances in which these system alerts are insufficient, such as users making sudden, brisk movements, like a forward jump. This has been the case with video games such as *Richie's Plank Experience*, which is designed to aid in combating the fear of heights. In certain cases, users have unintentionally jumped forward, breaking items around them and injuring themselves.[25] In other instances, applications that require fast arm movements, such as workout apps or boxing games, can lead to users inadvertently smacking objects, animals, or other people due to the energetic nature of the experience. Game developers have tackled this issue with pop-ups or warning screens when the virtual boundary set by the user is smaller than the recommended dimensions for the app in question. Additionally, headset developers have introduced updates to these boundary systems to detect when an object or person invades these preset boundaries and alert the user of their presence.

Stalking and Swatting

The use of location data can be vital for the core functionality of AR/VR products, as it will allow for location-based interactions and the use of certain safety measures, such as geofencing, a process in which a real-life location is assigned a virtual perimeter utilizing a device's GPS and data capabilities. But if bad actors compromise this data, it could put users at risk of stalking or other violent crime. Additionally, location data is susceptible to breaches at multiple points of the stack: Breaches can happen due to the presence of spyware in the devices, a lack of data stewardship by platforms, or even the users themselves when they unintentionally surrender their information in the heat of an online exchange.

For example, in the case of AR wearables, which are meant to be worn during significant portions of a user's day, if spyware were to be installed on the device, bad actors could observe the user's location by watching their surroundings through the device's cameras. Another example could be a user live streaming while using their AR glasses, inadvertently revealing details such as the street on which they reside or other sorts of personal information. In the case of MUIEs, users could disclose sensitive personal information while interacting with other users due to the fast-paced nature of voice chat. Unlike text-based communication, voice chat provides a frictionless form of conversation wherein a user has neither the chance to reread what they are sending nor the restraint of having to press a "send" button.

Concerns about unintentionally revealing location data of online users have been present for a long time and are relatively straightforward: If bad actors gain access to a user's location, they could stalk or physically threaten that user. Another potential harm is "swatting," wherein a person contacts law enforcement or other emergency services with a false claim that a violent crime is taking place in their residence.[26] This has become a more prominent practice in live streaming platforms such as Twitch, where streamers are usually targeted by ill-intentioned viewers who aim to see law enforcement break into the streamers' houses in the middle of their live streams.[27]

Another point of vulnerability in certain AR/VR products is the collection and storage of data created when these devices scan their surroundings to create a digital map stored either in-device or in the cloud—a process known as spatial mapping. This process is at the core of many AR/VR products. If bad actors were to compromise this information, it could give third parties the ability to "invert" the map, allowing them to digitally replicate the room the user is in and its layout. By having access to this information, a malicious actor—such as a stalker or a thief—could create a virtual replica of a room to pinpoint a user's location and take inventory of their possessions.[28] Map inversion is relatively unfeasible right now due to technological limitations, such as the quality of data captured by the devices and computational power for 3D deep-learning systems. There is a possibility that as devices' scanners improve and computational power increases in the future, these limitations will not be a restraint for those attempting to invert the maps.[29]

There are different ways to address the risk of stalking and swatting. Legislation can be a useful tool to deter these behaviors. While stalking is a crime everywhere in the United States, swatting is not. Some states, such as California, Michigan, and New Jersey, have recently enacted laws on swatting, but there is no federal law.[30] In other states, swatting falls under the false-reporting category, usually treated as a misdemeanor. Aside from legislation, police departments have started enacting antiswatting measures. One of them is Seattle's Rave Facility, an online registry individuals concerned with swatting can register with to help 911 operators. While registering in the system does not stop police forces from going to these locations, it allows emergency line operators to notify police forces of the swatting concern in hopes that this information might de-escalate the situation.[31]

Protecting users' location data will be another key factor in diminishing the risks of stalking and swatting and will require efforts from users themselves to standard setting organizations.

In the case of user error, the most effective measure will be tech literacy and establishing certain social norms in order to prevent users from unintentionally sharing personally identifiable information online. Live streaming platforms can also play an active role by displaying pop-ups or alerts to streamers using these devices to inform them of the potential risks of live streaming, such as disclosure of their location.

In the case of platforms, appropriate cybersecurity protocols might prevent data breaches or ransomware attacks that could let bad actors access users' location information. Additionally, product design and business models will also be an important factor. For example, platforms will need to consider whether spatial data will be shared with third parties and under what conditions. Another factor is a device's support for sideloading, a practice wherein users download and install applications through unsanctioned third-party app stores. Sideloading usually carries a higher risk of vulnerability to spyware and malware.[32]

Standard-setting boards will play a vital role in this realm, as they can aid platforms in establishing best practices, providing a roadmap and valuable insights over data stewardship and cybersecurity. Standard-setting organizations have already surfaced in AR/VR, such as the XR Safety Initiative (XRSI) and the Metaverse Standards Forum.[33] Policymakers can also aid in these efforts, as current privacy legislation is mainly at the state level, creating a costly patchwork of laws that introduce uncertainty for consumers and companies. A federal privacy law could provide necessary certainty, creating a single national standard regarding users' data rights and companies' data responsibilities.[34]

Leading Users to Locations That Are Dangerous or Off-Limits

Some AR products will allow users to interact with their physical environment by creating location-specific prompts or content. And while this technology provides various ways of creative expression and will enable users to consume location-specific content, there can be cases wherein it leads users to place themselves in dangerous situations or severely inconvenience nonusers who have not authorized the use of their property for these experiences.

One example of this is the popular mobile game *Pokémon GO*, which prompts players to walk around different locations to increase their collection of "Pokémon"—the game's flagship virtual animals—or meet up virtually in social spots knowns as "gyms" to compete with other players. The game's launch was incredibly successful, placing AR technology in the spotlight of the mainstream entertainment industry. But it also shed light on how these games could prompt users to go into dangerous, off-limit locations. For example, as the game launched, some gyms were located in high-security areas, such as the Pentagon.[35] There was also an instance where two men fell off from an 80-foot-high cliff while playing the game in Encinitas, California.[36] Other players repeatedly trespassed on private property in order to play the game.[37]

The developer behind the game, Niantic, responded to these issues by creating a reporting system that would allow individuals to report dangerous locations or ask to remove their property from the game. Additionally, it tweaked its gym and “Pokéstop” assignation system to prevent these spots from being located close to single-family homes, deleting pre-established stops that fit these criteria.

Pokémon GO provided a valuable lesson for developers in AR/VR who wish to deploy similar technology. While location-based experiences can be immensely beneficial, the location assignment cannot be done entirely randomly, and it needs to be accompanied by a robust reporting system to keep both users and nonusers safe. Additionally, developers can use tools such as geofencing to deactivate its services in dangerous or classified areas.

Inciting Violence or Vandalism

Online platforms have allowed millions of individuals to have a platform in which they can exchange ideas and interact with each other. But while it has allowed for a democratization of information and provided a platform for unprecedented creative expression, it has also given a platform to speech that could lead to physical harm.[38]

There are instances when content can lead to the rise of potentially life-threatening situations for both users and nonusers. One example of this can be during public safety emergencies, such as the escalation of a national protest. Such was the case in Colombia in 2019, where a hoax in the middle of a nationwide protest led residents of Cali and Bogotá to believe that protestors were breaking into and looting houses in certain neighborhoods. As there had been some prior confrontation between protesters and law enforcement officers, this hoax was rapidly believed and spread, driving the population into widespread panic, with numerous groups of civilians armed with blunt force weapons and firearms started patrolling their neighborhoods, sometimes targeting innocent bystanders whom they had mistakenly labeled as looters. It also caused a massive spike in calls to the local emergency lines, which caused confusion among law enforcement and diminished its capacity to respond to actual security threats.[39]

Platforms have developed different tools to respond to these kinds of threats. One of them is flagging problematic words or content with advisories that can correct the false information. But the use of these tools creates two problems for platforms: It requires them to be able to sort through the noise and have access to the “actual” truth, which is not always possible in these fast-paced scenarios. They also need to have the technical means to create a system to decide which content to flag, which usually requires the use of automated systems that are not always accurate and can be exploitable. Another option is to remove content, but that presents similar issues to those previously mentioned. Finally, platforms can throttle or limit the capacity of users to submit content related to a topic or any content at all during specific periods of time. Aside from the technical issues mentioned before, this option can be particularly risky for platforms, as it can cause them to inadvertently be perceived as “picking sides,” thus reducing user trust and potentially further escalating the issue, as animosity could rise among throttled users.

Health Misinformation

Misinformation is another example of online content that can easily translate to serious harm in the physical realm. One example of this phenomenon is the infamous “Tide pod challenge,” a viral social media trend in which users prompted others to ingest a laundry detergent pod.[40] But while this was a relatively straightforward topic in which the harm was largely indisputable, there are other instances when the information is not readily available to platforms or is rapidly changing. For example, the COVID-19 pandemic posed a particularly difficult challenge for platforms, as they attempted to make life-saving information readily available to their users but had to prevent the spread of misinformation.

For such straightforward cases, platforms employ multiple tools to detect and take down content in a timely manner. For example, they can simply remove all content that contains a particular phrase or hashtag directly related to the matter. They can also employ artificial intelligence tools to screen, flag, or remove harmful content. The challenge for platforms is primarily technical: figuring out the best method to filter content to find harmful content promptly and accurately. As previously mentioned, content moderation will become more difficult in MUIEs due to the various forms of expression present, making content screening more difficult. Platforms that rely on a more decentralized approach to content moderation will benefit from some content moderation being done at the community level, although that comes with the risk community moderators might not align with the company values.

Finding misinformation becomes particularly difficult when information is not readily available. In such cases, platforms must not only go through the task of determining the best technical tools, but also sort through rapidly changing information. Nonetheless, platforms might benefit from the fact that MUIEs, in their current form, tend to have a more compartmentalized structure, as users have to hop on and off from worlds or rooms. This compartmentalization might decrease the speed at which speech travels in MUIEs, which might slow down the spread of misinformation compared with most 2D social media.

Immersive Haptics and Sexual Violence

Most AR/VR products target a general audience, usually aiming at gaming, social media, and enterprise users. But as the technology matures, some of its more-specific applications, such as products designed for sexual use, might become more prominent. With a topic as personal and sensitive as sexual intimacy, any potential risks that could lead to nonconsensual interactions could be tremendously harmful to the affected users.

The Australian eSafety commissioner has expressed increased concerns over the potential for groping or other sexual assaults when users wear a haptic suit. The commissioner has also warned of the potential for nonconsensual activity with immersive sexual devices (e.g., if the user controlling the device is a nonauthorized user, which can happen if the device has been hacked or is shared without the other users’ permission).[41] Due to the novelty of these devices and their niche application, discussion on the topic has been scarce. Thus, most of the responsibility to confirm the identity of the person controlling the device falls on the users that are part of the interaction.

Mental Harms

Sexual Violence in MUIEs

AR/VR technology allows for new methods of online interaction—particularly in MUIEs, where users have access to both verbal and nonverbal communication. MUIEs allow more robust social interaction, amplifying the emotions and impact of online speech compared with their 2D counterparts. But in the same way these tools can amplify positive and desirable interactions, they can also make negative experiences way more impactful for users.

Online platforms already have to deal with the issue of sexual harassment, as it has been present in social media, multiplayer video games, and avatar-based multiplayer experiences. But the immersive nature of MUIEs and their use of AR/VR tools make these negative encounters potentially more impactful for users and, therefore, more damaging.[42] As these online platforms grow in popularity and relevance, there have been complaints about the potential for new types of virtual sexual violence in these immersive experiences.

One of the most common sexually violent behaviors in MUIEs is virtual groping and harassment.[43] An incident of virtual groping among beta testers of Meta's platform *Horizon Worlds* brought awareness of the potential issue of players using the ability to express nonverbal language—such as leveraging the device's ability to mimic hand movement accurately—to sexually harass other users.[44] In the early stages of these platforms, users will sometimes use their avatars to block other users from moving, essentially cornering them into a wall or blocking an exit.[45]

In response, Meta introduced a personal boundary system, which erects a four-foot virtual barrier around avatars, thereby preventing other users from invading their personal space by pushing their avatars aside. Additionally, when other users intend to extend their hands into this boundary, their hands will fade out of the picture until they leave the boundary area. Meta has also placed a strong emphasis on certain traditional personal safety tools, such as blocking and muting, that allow for a quicker response against abusive behavior than does waiting for first-party moderators to step in. Additionally, Meta has introduced a tool unique to MUIEs named "safe zone," in which users can quickly exit their virtual world to be introduced into a safe, empty world to escape stressful situations rapidly. While in this safe zone, users can still block or mute players they had recently interacted with. Other MUIE platforms, such as VRChat or AltSpaceVR*,* have enacted similar systems.

Cyberbullying and Virtual Harassment

Another problem in AR/VR spaces is cyberbullying and harassment, which have been recurrent concerns in social media and have already shown up in AR/VR spaces.[46] While conversations around cyberbullying tend to focus on teenagers, this is an issue that can also affect adults. Concerns over harassment and bullying are common in the gaming community, which tends to overlap with the current user base of AR/VR platforms.[47]

Some of the personal safety tools previously mentioned, particularly safe zones, will allow for quick de-escalation of situations involving bullying or harassment, as users will be able to escape stressful situations quickly and have an environment that provides time and space to take the measures they deem necessary. But individual content moderation tools might not be enough to deter antisocial behavior. Enacting legislation that codifies cyberbullying as a crime could be a productive measure to tackle the issue, providing an additional deterrence to hostile users.[48]

Harmful Content

As online 2D platforms have grown in popularity and become a mainstream method of communication, there have been increasing concerns about the spread of potentially harmful content and the potential negative impact certain social media platforms could have on teenagers' body image.[49] Other examples of problematic content include the glorification of drug use, eating disorders, and self-harm. There is a concern that harmful content and behavior will tend to leave the virtual realm and lead to tangible harm to users' mental health.[50]

These problems are likely to resurface in MUIEs due to the increased difficulties regarding content moderation in these spaces. Content moderation at scale in these platforms will pose a technical and economic challenge due to the fast pace and variety of speech in MUIEs, with interactions that happen in real time often being ephemeral and heavily reliant on nonverbal communication—and moderation will introduce new privacy dilemmas.[51] Traditional tools currently used to thwart harmful content, such as pop-ups for specific search terms or content filters, will probably be less effective in MUIEs because most communication is not written and users will not be using search bars as often as they do in 2D social media.[52] Most MUIEs, due to their decentralized approach in which each world or room creates a "silo," will also be able to leverage community-driven content moderation systems in which both community moderators and the individual users can mute, block, or kick out undesirable individuals.[53]

Addiction and Psychological Impact of Virtual Socialization

As with most new technologies, particularly those that cause brain stimulation (e.g., video games, cell phones) there is concern over the impact of AR/VR on users' mental health. Some people have even labeled AR/VR products as a "technological drug" that can cause severe addiction among its users.[54] There are also additional concerns regarding the prevalence of antisocial behavior in MUIE platforms, which could translate to antisocial behavior in the physical world. There are fears that continuous exposure to undesirable behavior might desensitize users.[55] But as has happened in the past with social media and other technologies, most of the claims regarding the potential psychological harms of AR/VR tech, such as its addictiveness or relation to poor mental health, are exaggerated and lack scientific consensus.[56]

Nonetheless, platforms have taken numerous steps to tackle any potential harms, with measures such as allowing users to limit their screen time and see screen-time reports, or by notifying them to take a break whenever they have spent a certain amount of time on an app. Additionally, content warnings such as the ones established by ESRB will allow users to be aware of content that might trigger any sensibilities. While such a standard is more challenging to implement in MUIEs, 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.

Financial Harms

Gambling

As online gambling has been on the rise in recent years, it is expected to have a presence in AR/VR technology. A clear example of this is the *Pokerstars VR* app, which allows users to play poker, blackjack, and slots on the platform. As a free-to-play app, users start with an allotted amount of in-game currency, which regenerates over time, and can buy more credits when they run out. Due to the impossibility of "cashing out" earnings, this free-to-play model falls under the category of simulated gambling. Even in simulated experiences, betting and gambling introduces some risks for users, as it is an activity that can lead to addiction. Gambling is a particularly damaging addiction and can direct users to make decisions that could financially cripple them.

With the rising popularity of online sports betting, it is expected that AR/VR devices will support and carry betting apps in the future. There are projects under way to create AR/VR casinos, which will create MUIEs that will place users in virtual casinos where they can bet on different games and sports, socialize with other bettors, and watch live sports in a way that resembles physical casinos. Current offerings are limited to the free-to-play model, but that might change in the future.[57]

Current experiences with the recent liberalization of sports betting in most states will provide a roadmap for adopting these products. Initially, the transition from the smartphone world into AR/VR should find little difficulties, as current regulations should be applicable in AR/VR. Some of the age-verification measures existing in smartphone apps—such as ID verification—are likely to face practical challenges in their transition to standalone AR/VR devices, such as the ability to scan a user's ID with a device's camera. Still, in the early stages of the transition, they can rely on users' smartphones as they develop AR/VR-ready tools. For example, developers can use a companion smartphone app that is able to scan and process the ID scan, thereby preventing a user from accessing the content until the scan has been completed. Additionally, policymakers can demand developers provide resources for users facing gambling issues, such as including items or notices in their worlds that provide users with information about the available resources and hotlines to combat gambling addiction.

Identity Theft, Fraud, and Ransomware

Most general use AR/VR products aim to be a central part of the metaverse, a concept used to describe the online world that most Web 3.0 projects try to create. In the metaverse, users will be able to craft an identity unique to their online experience, usually represented in their avatars, possession of different digital assets, and presence and role in virtual social experiences, among other ways of expression online. The synergy between AR/VR and other Web 3.0 technologies (e.g., nonfungible tokens (NFTs) and cryptocurrencies) will likely lead to the creation of a vast online economy. In this vision of the online world, users will buy and sell various digital goods, spending significant amounts of their money in these online markets. While this provides an avenue for limitless personal expression, protecting these digital assets will become a concern for users.

Online video games can shed light on the potential risks for users, as this is an issue that has existed in the space for decades. This was the case in the early years of multiplayer online role-playing games, in which users could trade items with each other, and phishing and different sorts of fraud were common. Bad actors would trick users into forfeiting their login credentials and then transfer all their items out of their accounts.[58] As in-game transactions had not become popularized yet, losing in-game items usually represented merely a loss of time for users. But as the online gaming market has matured, video games now host a more significant number of bought items. This transition has led the industry to use different measures to secure users' digital inventories.

In some cases, these games have restricted the ability of players to trade items altogether. Doing so prevents these bad actors from "profiting" from transferring these items to themselves, as the items are permanently linked to the account that bought them. While effective for those who want to profit off these items, this measure does little to prevent ransomware attacks, which aim to ask users for a ransom to return their accounts to their possession. In these cases, restricting the ability to trade will be of no help to the affected users. This is an instance when two-factor authentication can be particularly helpful, preventing these bad actors from logging into a user's account. Additionally, another tool at the disposal of AR/VR companies is support for password managers, which will incentivize users to use stronger, more-unique passwords that tend to be more difficult to guess and less susceptible to compromise in the case of a data breach. In the long run, these technologies might adapt beyond the use of passwords and face scans and implement new methods of identity verification, such as zero-trust authentication (ZeTA), wherein users answer a series of questions based on a secret they have learned (e.g., If the secret is "red AND round" they might answer yes to "apple?" but no to "fire truck?").[59]

Impersonation and Reputational Damage

As AR/VR devices and the social platforms surrounding them aim to blur the lines between the digital and the physical world, impersonation can become a serious threat in the metaverse. With the increasing development of tools to create deepfakes, impersonation can cause an individual tremendous professional and personal damage by ruining their reputation.[60] For example, someone can use a deepfake tool to create an avatar that resembles a person and record themselves using offensive expressions. These actions could have real-world consequences for individuals who be fired from their jobs or excluded from their communities.

Impersonation is a difficult issue to tackle on social media. Verifying a user's identity upon enrollment can reduce impersonation but creates a trade-off with anonymity valued by other users, such as those in marginalized communities or residing in authoritarian regimes.[61] As a method to tackle the issue, social media platforms have established impersonation report systems that allow users to report when someone impersonates them, but as with content moderation systems, these might face enforcement difficulties at scale.[62] While MUIEs do not currently support photorealistic avatars, this concern could arise in the future. A potential method to prevent impersonation with avatar deepfakes could be restricting the use of photorealistic avatars to those willing to verify their identity with a face scan or by forcing them to take a selfie. This measure would allow users to use realistic avatars, while avoiding some of the privacy concerns associated with ID verification. Optional identity verification has been successfully implemented in dating apps, which have benefited from the increased trust inherent to their users being "verified," while still respecting the privacy concerns of skeptical users.[63]

RECOMMENDATIONS

Scrutiny of AR/VR technology and its associated products is going to be vital to ensure the technology provides a safe experience to users and that companies promptly address any mistakes. Policymakers will have a role in this process, especially in ensuring what is illegal in the physical world is also illegal in the virtual one. They can also fund research to address concerns about physical and psychological safety.

Consider the Impact of Laws and Regulations for Internet Platforms on AR/VR

Policymakers should consider the impact that proposed laws and regulations for Internet platforms, such as laws for social media and biometrics, could have on the development of AR/VR. Policymakers should be mindful that they consider how these proposals could stifle innovation in a market that has yet to mature. For example, consider proposals that aim to increase intermediary liability for user-generated content, as most reforms to Section 230 of the Communications Decency Act would do. MUIEs will be heavily reliant on user-generated content, as users will be the ones crafting most of the worlds in which other users will interact. In these spaces, user-generated content will take multiple shapes and forms and, as described throughout this report, will be more challenging to monitor and moderate. If AR/VR platforms were to be liable for the content created by their users, their products would become inherently riskier, as any missteps in their content moderation system could translate into a costly lawsuit. This legal risk would translate into higher costs for consumers, as well as make it prohibitively expensive for new businesses to enter the market, thereby hindering competition.[64]

In a young market such as that of AR/VR, having the ability to experiment with new technologies and processes freely is vital to innovation. And while this experimentation has the potential to be incredibly beneficial for consumers, it also brings inherent risks. Companies will experiment with different safety tools at both the individual level and the platform level in order to define an appropriate safety toolkit, and experimentation inherently brings a risk of failure. Policymakers should abstain from interfering with the process that takes place in these developing markets and allow market participants to experiment freely—and limit interventions to situations when the market has proven incapable of providing a solution and there is demonstrable harm to users.

Criminalize Harmful Behaviors That Impact AR/VR Safety at the Federal Level

There are other areas that might benefit from government intervention where the market process has shown to be insufficient or that might just be outside its realm (e.g., the codification of certain digital crimes). Due to its novelty and relatively niche nature, virtual sexual violence has often been disregarded as a serious offense. But as digital identities become more relevant in day-to-day life, it is essential that certain crimes, such as “revenge porn” or online fraud schemes, are taken seriously by law enforcement. Doing so will require new laws banning this behavior and educating law enforcement so they are aware of how some of these online harms can easily translate into tangible real-world harms. Similarly, current legislation against bullying currently focuses on behavior that takes place inside school property, and in some cases, it does not even consider bullying as a crime. Setting appropriate and proportional punishments for offenders might prevent this undesirable behavior from happening in the first place, and will provide recourse for victims.[65]

Tackling these issues will require efforts from different agencies and actors in government. As an initial step, Congress should enact federal legislation that codifies behavior such as cyberbullying, distributing revenge porn, and swatting as a crime across all 50 states. The proposed Online Safety Modernization Act, introduced in 2017, aims to tackle some of these issues but has gained little traction since its introduction.[66]

Create Best Practices for State and Local Law Enforcement Agencies

Alongside legislation, the Department of Justice should look into creating guidelines for local and state police departments that raise awareness of cybercrimes in AR/VR, and provide tools for police officers to respond accordingly. Online sexual violence and fraud need to be taken seriously by law enforcement agencies in the first place to trigger a proper response. In the case of swatting, establishing best practices and reporting systems—such as Seattle's Rave Facility—could help de-escalate the situation, potentially reducing the harm of these false calls.

Establish Federal Safety Guidelines for HUDs

Government agencies can also play a valuable role in consumer protection and standard-setting processes. For example, NHTSA issued driver distraction guidelines for in-vehicle electronic devices in 2014, which set forward a standard for the introduction of in-vehicle screens present in many current vehicles.[67] And while these guidelines have been influential in the development of heads-up displays in vehicles so far, updating these guidelines to address AR/VR-specific issues would provide a more streamlined adoption process in a safe manner. NHTSA announced that HUDs would likely be covered in the proposal second phase of the guidelines, but this update has yet to be issued.[68] Additionally, the Federal Trade Commission's Consumer Protection Bureau should monitor potential fraudulent activity in the metaverse in order to swiftly respond to any new methods of cyber fraud that might arise in the space.

Fund User Safety Research

Finally, the government could be a powerful catalyst for research that helps answer unknown questions, which can provide much needed certainty over the safety of AR/VR products. As previously mentioned, most of the concerns regarding the psychological harms surrounding the continued use of AR/VR (e.g., its addictiveness) lack scientific consensus. Additional research could provide definitive answers to a concern that seems to have contradicting information. Agencies such as the National Institutes of Health should provide grants to promote research on the matter.

Another issue that could benefit from additional research is a further look into the causes and possible mitigation techniques for some of the physical issues previously exposed herein, such as eye strain and motion sickness. The Department of Labor, through agencies such as the Employment and Training Administration and the Occupational Safety and Health Administration, should make bolstering research on those two issues a priority. As AR/VR tech is increasingly implemented in training programs and productive processes, workers will be using these devices over long periods of time. Research that looks into methods to mitigate any adverse physical effects would benefit those government employees that will be using these devices, and can potentially shed light on new best practices.[69]

CONCLUSION

As AR/VR technology aims to impact a broad range of fields, the definition of user safety in extended reality requires broadening to encompass psychological and financial safety instead of merely physical safety. Guaranteeing a safe experience for AR/VR users will require the work of different actors in the space, from developers to users and community leaders to policymakers. AR/VR has been heavily influenced by various past technologies, such as video games, social media, and smartphones. This allows these actors to tap into the vast amount of knowledge over what tools are helpful to tackle the different threats that are present—or could potentially be present—in AR/VR products.

As with most novel technologies, addressing concerns regarding user safety will require experimentation with different tools and approaches. That experimentation process will lead certain companies to take missteps. Policymakers and regulators need to be conscious of experimentation as a driver of innovation and development in young markets. They should be wary of regulations that could potentially stifle developers' and platforms' ability to experiment freely. Instead, there are certain aspects in which government could help spur innovation in the field, such as looking into federal-level privacy legislation or codifying certain digital crimes.

About the Author

Juan Londoño is a policy analyst focusing on augmented and virtual reality at the Information Technology and Innovation Foundation. Prior to joining ITIF, Juan worked as a tech and innovation policy analyst at the American Action Forum, where his research focused on antitrust, content moderation, AR/VR, and the gaming economy. Juan holds an M.A. in Economics from George Mason University and a B.A. in Government and International Relations from the Universidad Externado de Colombia.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent, nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized by its peers in the think tank community as the global center of excellence for science and technology policy, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. For more information, visit us at itif.org.

ENDNOTES

1. "What is Online Safety?" South West Grid for Learning, accessed 05/11/2022, https://swgfl.org.uk/online-safety/what-is-online-safety/.
2. "ITIF Technology Explainer: What Is AR/VR?" (ITIF, November 18, 2020), https://itif.org/publications/2020/11/18/itif-technology-explainer-what-arvr.
3. Rose Eveleth, "Google Glass Wasn't a Failure. It Raised Crucial Concerns," *Wired*, accessed 04/25/2022, https://www.wired.com/story/google-glass-reasonable-expectation-of-privacy/.
4. Adam Thierer, "The Great Facial Recognition Technopanic of 2019," *The Bridge*, accessed 12/05/2022, https://www.mercatus.org/bridge/commentary/great-facial-recognition-technopanic-2019.
5. Ellysse Dick, "Smart Glasses Have Arrived. Congress Needs to Catch Up," *Morning Consult*, September 13, 2021, https://morningconsult.com/opinions/smart-glasses-have-arrived-congress-needs-to-catch-up/.
6. Alex Heath, "Mark Zuckerberg's augmented reality," *The Verge*, accessed 11/14/2022, https://www.theverge.com/23022611/meta-facebook-nazare-ar-glasses-roadmap-2024.
7. Damon Lavrinc, "Google Glass Could Be Banned for Drivers in West Virginia," *Wired*, accessed 04/06/2022, https://www.wired.com/2013/03/google-glass-ban-west-virginia/.
8. Laura Walter, "Can You Safely Walk and Listen to Music at the Same Time?" *EHSToday,* accessed 11/14/2022, https://www.ehstoday.com/safety/article/21912591/can-you-safely-walk-and-listen-to-music-at-the-same-time; Stefania Barbieri et al., "Pedestrian Inattention Blindness While Playing Pokémon Go as an Emerging Health-Risk Behavior: A Case Report," *Journal of Medical Internet Research* vol. 19,4 e86, April 1, 2017, doi:10.2196/jmir.6596.
9. Robert Eveson, "Redes sociales: blessing or curse?" Latin America Bureau, accessed 04/21/2022, https://lab.org.uk/redes-sociales-blessing-or-curse/.
10. Lindsey Bever, "Teens are daring each other to eat Tide pods. We don't need to tell you that's a bad idea," *The Washington Post*, accessed 04/21/2022, https://www.washingtonpost.com/news/to-your-health/wp/2018/01/13/teens-are-daring-each-other-to-eat-tide-pods-we-dont-need-to-tell-you-thats-a-bad-idea/.
11. Mark Jamison and Matthew Glavish, "The dark side of the metaverse, part I," *AEIDeas*, March 17, 2022, https://www.aei.org/technology-and-innovation/the-dark-side-of-the-metaverse-part-i/.
12. Joshua New, "Comments to the U.S. Consumer Product Safety Commission on the Internet of Things and Consumer Product Hazards" (ITIF, July 31, 2019), https://itif.org/publications/2019/07/31/comments-us-consumer-product-safety-commission-internet-things-and-consumer/.
13. 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.
14. Heath, "Mark Zuckerberg's Augmented Reality."
15. "Distracted Driving," Governors Highway Safety Association, accessed 11/01/2022, https://www.ghsa.org/state-laws/issues/distracted%20driving.
16. Bill Chappell, "Honolulu's 'Distracted Walking' Law Takes Effect, Targeting Phone Users," *NPR*, accessed 04/07/2022, https://www.npr.org/sections/thetwo-way/2017/10/25/559980080/honolulus-distracted-walking-law-takes-effect-targeting-phone-users.
17. Lavrinc, "Google Glass Could Be Banned for Drivers in West Virginia."

18. Fred Meiert, “Which Cars Have Head-Up Displays?” Cars.com, accessed 11/02/2022, https://www.cars.com/articles/which-cars-have-head-up-displays-434824/; Lawrence Ulrich, “Head-Up Car Displays Coming in 2024>Mass-market players will introduce HUD-enabled driving soon,” *IEEE Spectrum*, accessed 11/02/2022, https://spectrum.ieee.org/augmented-reality-car-hud.

19. Preshit Deorukhkar, “How to Cut Down Notifications and Minimize Distractions with Focus on iOS 15,” *Readdle,* accessed 04/26/2022, https://readdle.com/blog/how-to-focus-mode-ios; Florence Ion, “How to Set Up Focus Mode on Android and iOS,” *Gizmodo*, accessed 11/02/2022, https://gizmodo.com/how-to-set-up-focus-mode-android-ios-samsung-schedule-1849602887/slides/3.

20. Joseph J. LaViola, “A discussion of cybersickness in virtual environments,” *SIGCHI Bull. 32, 1,* January, 2000, 47–56. DOI: https://doi.org/10.1145/333329.333344.

21. Andras Kemeny, Jean-Rémy Chardonnet, and Florent Colombet. *Getting Rid of Cybersickness: In Virtual Reality, Augmented Reality, and Simulators*. Cham: Springer International Publishing AG, 2020.

22. Christine Romans, “Is Virtual Reality Bad for Your Eyes?” *Make Use Of,* accessed 05/09/2022, https://www.makeuseof.com/virtual-reality-bad-your-eyes/.

23. “Eyestrain,” Mayo Clinic, accessed 05/09/2022, https://www.mayoclinic.org/diseases-conditions/eyestrain/symptoms-causes/syc-20372397.

24. Sarah E. Needleman and Salvador Rodriguez, “VR to the ER: Metaverse Early Adopters Prove Accident-Prone,” *The Wall Street Journal,* accessed 11/14/2022, https://www.wsj.com/articles/metaverse-virtual-reality-vr-accident-prone-meta-11643730489; Shannen Camp, “People Who Got Seriously Hurt Playing Vr Games,” *SVG,* accessed 11/15/2022, https://www.svg.com/156530/people-who-got-seriously-hurt-playing-vr-games/?utm_campaign=clip; John Ely, “German gamer, 31, breaks his NECK because of his ‘repetitive’ and ‘intense’ movements using a VR headset,” *Daily Mail*, accessed 11/15/2022, https://www.dailymail.co.uk/health/article-10033285/German-gamer-breaks-NECK-using-VR-headset.html.

25. “Dad Breaks TV Virtual Reality FAIL,” Twitter Posts, accessed 04/06/2022 https://youtube.com/shorts/fNKBqx5mNjI.

26. “Call of Duty ‘swatting’ death prankster pleads guilty,” *BBC*, accessed 04/28/2022, https://www.bbc.com/news/technology-46206616.

27. Jeremy Winslow, “Hearthstone Streamer Swatted Live On Twitch,” *Kotaku*, accessed 04/28/2022, https://kotaku.com/twitch-hearthstone-streamer-police-swat-arrested-allies-1848522725.

28. Francesco Pittaluga et al., “Revealing Scenes by Inverting Structure from Motion Reconstructions,” *arXiv:1904.03303v1* (5 Apr 2019), DOI: https://doi.org/10.48550/arXiv.1904.03303.

29. Jaybie Agullo de Guzman, Aruna Seneviratne, and Kanchana Thilakarathna, “Unravelling Spatial Privacy Risks of Mobile Mixed Reality Data.” Proceedings of ACM on interactive, mobile, wearable and ubiquitous technologies 5, no. 1 (2021): 1–26.

30. Victim Connect, “Stalking,” Victim Connect, accessed 11/03/2022, https://victimconnect.org/learn/types-of-crime/stalking/; John R. Vile, “Swatting,” The First Amendment Encyclopedia, accessed 11/03/2022, https://www.mtsu.edu/first-amendment/article/1578/swatting.

31. “Protect Yourself from Swatting,” Seattle Police Department, accessed 11/02/2022, https://www.seattle.gov/police/need-help/swatting.

32. Jennifer Huddleston and Juan Londoño, “Does “Sideloading” Strengthen Competition on Mobile Devices? “ American Action Forum*,* March 3, 2021, https://www.americanactionforum.org/insight/does-sideloading-strengthen-competition-on-mobile-devices/.

33. "The XRSI Privacy and Safety Framework 2," XR Safety Initiative, accessed 05/04/2022, https://xrsi.org/the-xrsi-privacy-and-safety-framework-2; "Leading Standards Organizations and Companies Unite to Drive Open Metaverse Interoperability" Metaverse Standards Forum, accessed 11/02/2022, https://metaverse-standards.org/news/press-releases/leading-standards-organizations-and-companies-unite-to-drive-open-metaverse-interoperability/.

34. Dick, "Balancing User Privacy and Innovation in Augmented and Virtual Reality."

35. "'Pokemon Go': 10 Strangest Pokestop Locations," *Rolling Stone*, accessed 11/03/2022, https://www.rollingstone.com/culture/culture-lists/pokemon-go-10-strangest-pokestop-locations-14745/the-pentagon-210003/.

36. David Hernandez, "'Pokemon Go' players fall off 90-foot ocean bluff," *The San Diego Union-Tribune,* accessed 11/03/2022, https://www.sandiegouniontribune.com/sdut-pokemon-go-encinitas-cliff-fall-2016jul13-story.html.

37. Ivy Taylor, "Niantic agrees to combat trespassing Pokémon Go players," *GamesIndustry.biz*, accessed 04/29/2022, https://www.gamesindustry.biz/articles/2019-09-06-niantic-agrees-to-combat-trespassing-pok-mon-go-players.

38. Daniel Castro, "Content Moderation in Multi-User Immersive Experiences: AR/VR and the Future of Online Speech" (ITIF, February 28, 2022), https://itif.org/publications/2022/02/28/content-moderation-multi-user-immersive-experiences-arvr-and-future-online.

39. "Los mensajes falsos que generaron la ola de pánico en Bogotá y Cali, ¿por qué nos los creímos?" *El Espectador*, https://www.elespectador.com/colombia/mas-regiones/los-mensajes-falsos-que-generaron-la-ola-de-panico-en-bogota-y-cali-por-que-nos-los-creimos-article-892605/.

40. Bever, "Teens are daring each other to eat Tide pods."

41. "Immersive technologies – position statement," Australian eSafety Commissioner, accessed 05/02/2022, https://www.esafety.gov.au/industry/tech-trends-and-challenges/immersive-tech.

42. Raymond Lavoie et al., "Virtual experience, real consequences: the potential negative emotional consequences of virtual reality gameplay." *Virtual Reality 25,* (2021), 69–81, https://doi.org/10.1007/s10055-020-00440-y.

43. Castro, "Content Moderation in Multi-User Immersive Experiences.".

44. Tanya Basu, "The metaverse has a groping problem already," *MIT Technology Review*, accessed 05/02/2022, https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/.

45. Adi Robertson, "Meta is adding a 'personal boundary' to VR avatars to stop harassment," *The Verge*, accessed 05/03/2022, https://www.theverge.com/2022/2/4/22917722/meta-horizon-worlds-venues-metaverse-harassment-groping-personal-boundary-feature.

46. Robert D. Atkinson et al., "A Policymaker's Guide to the 'Techlash'—What It Is and Why It's a Threat to Growth and Progress" (ITIF, October 28, 2019), https://itif.org/publications/2019/10/28/policymakers-guide-techlash/; Sheera Frenkel and Kellen Browning, "The Metaverse's Dark Side: Here Come Harassment and Assaults," *The New York Times*, accessed 11/04/2022, https://www.nytimes.com/2021/12/30/technology/metaverse-harassment-assaults.html.

47. Kellen Browning, "More Resignations, but No Sign Yet of a Change in Gaming Culture," *The New York Times*, accessed 11/04/2022, https://www.nytimes.com/2020/07/19/technology/gaming-harassment.html.

48. Atkinson et al., "A Policymaker's Guide to the 'Techlash'—What It Is and Why It's a Threat to Growth and Progress."

49. Georgia Wells, Jeff Horwitz, and Deepa Seetharaman, “Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show,” *Wall Street* Journal, accessed 05/03/2022, https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739.

50. Juan Londoño, “Lessons from Past Technopanics for Current Social Media Debates,” *American Action Forum,* October 28, 2021, https://www.americanactionforum.org/insight/lessons-from-past-technopanics-for-current-social-media-debates/; “‘Thousands of messages a day’: New York Times reporter reveals toll of online abuse,” *MSNBC,* accessed 05/04/2022, https://www.msnbc.com/american-voices/watch/-thousands-of-messages-a-day-new-york-times-reporter-reveals-toll-of-online-abuse-132042821695.

51. Juan Londoño, “Lessons from Social Media for Creating a Safe Metaverse” (ITIF, April 28, 2022), https://itif.org/publications/2022/04/28/lessons-social-media-creating-safe-metaverse.

52. “Suicide and Self Injury,” *Meta*, accessed 05/05/2022, https://transparency.fb.com/policies/community-standards/suicide-self-injury/.

53. Castro, “Content Moderation in Multi-User Immersive Experiences: AR/VR and the Future of Online Speech” ; Anne Hobson, “Phantoms, Crashers, and Harassers: Emergent Governance of Social Spaces in Virtual Reality,” Center for Growth and Opportunity, July 2020, https://www.thecgo.org/wp-content/uploads/2020/09/Phantoms-Crashers-and-Harassers-Emergent-Governance-of-Social-Spaces-in-Virtual-Reality.pdf.

54. “Is virtual reality an addictive drug?” *BBC,* accessed 05/05/2022, https://www.bbc.com/news/blogs-echochambers-27264418.

55. Michael Pittaro, “Exposure to Media Violence and Emotional Desensitization,” *Psychology Today*, accessed 05/05/2022, https://www.psychologytoday.com/us/blog/the-crime-and-justice-doctor/201905/exposure-media-violence-and-emotional-desensitization; Yasaman Farazan, “Breaking the Virtual Ice: Antisocial Behaviors in Social Virtual Reality and How Developers Cope with Them,” ResearchGate, February 2021, https://www.researchgate.net/publication/349212255_Breaking_the_Virtual_Ice_Antisocial_Behaviors_in_Social_Virtual_Reality_and_How_Developers_Cope_with_Them; “New research shows Metaverse is not safe for kids,” Center for Countering Digital Hate, Dec 30, 2021, https://www.counterhate.com/post/new-research-shows-metaverse-is-not-safe-for-kids.

56. Farhad Manjoo, “The Moral Panic Engulfing Instagram,” *The New York Times,* accessed 05/05/2022, https://www.nytimes.com/2021/10/13/opinion/instagram-teenagers.html; Londoño, “Lessons from Past Technopanics for Current Social Media Debates”; David Moschella, “Living Online Is a Societal Phase, Not a Dangerous Addiction” (ITIF, October 31, 2022, https://itif.org/publications/2022/10/31/living-online-is-a-societal-phase-not-a-dangerous-addiction/.

57. XR Casino, Inc. “XR Casino Aims to Disrupt Online Gambling and Sports Betting Industries through Augmented Reality (AR), Mixed Reality (MR) and Virtual Reality (VR) Technologies,” *Globe Newswire,* accessed 05/05/2022, https://www.globenewswire.com/en/news-release/2021/07/09/2260569/0/en/XR-Casino-Aims-to-Disrupt-Online-Gambling-and-Sports-Betting-Industries-through-Augmented-Reality-AR-Mixed-Reality-MR-and-Virtual-Reality-VR-Technologies.html.

58. “Scams,” The Runescape Wiki, accessed 11/03/2022, https://runescape.fandom.com/wiki/Scams.

59. VentureBeat, “Passwords May Get Replaced For VR Devices By Zero-Trust Authentication,” *UploadVR*, accessed 11/04/2022, https://uploadvr.com/passwords-zero-trust-authentication-vr/.

60. Carolyn Pepper, “Lawyer: What to do about deepfake and metaverse libel threat to publishers,” *PressGazette,* accessed 11/04/2022, https://pressgazette.co.uk/deepfake-metaverse-publishers/.

61. Derek du Preez, “ID verification for social media as a solution to online abuse is a terrible idea” Diginomica, accessed 11/04/2022, https://diginomica.com/id-verification-social-media-solution-online-abuse-terrible-idea.

62. “Report impersonation accounts” Twitter, accessed 11/04/2022, https://help.twitter.com/en/safety-and-security/report-twitter-impersonation; Oana Goga et al., “The Doppelgänger Bot Attack: Exploring Identity Impersonation in Online Social Networks,” *Proceedings of the 2015 Internet Measurement Conference* (2015): 141–153, https://doi.org/10.1145/2815675.2815699.

63. Daniel Van Boom, “Tinder ID verification lets you prove you are who you say you are,” *Cnet,* accessed 11/04/2022, https://www.cnet.com/culture/tinder-id-verification-lets-you-prove-you-are-who-you-say-you-are/.

64. Juan Londoño, “The Erosion of Intermediary Liability Protections Can End the Metaverse Before It Even Starts” (ITIF, March 17, 2022, https://itif.org/publications/2022/03/17/erosion-intermediary-liability-protections-can-end-metaverse-it-even-starts.

65. Atkinson et al., “A Policymaker’s Guide to the ‘Techlash'—What It Is and Why It’s a Threat to Growth and Progress.”

66. H.R.3067 - Online Safety Modernization Act of 2017, accessed 11/15/2022, https://www.congress.gov/bill/115th-congress/house-bill/3067.

67. “Visual-Manual NHTSA Driver Distraction Guidelines for In-Vehicle Electronic Devices,” National Highway Traffic Safety Administration, accessed 11/15/2022, https://www.federalregister.gov/documents/2014/09/16/2014-21991/visual-manual-nhtsa-driver-distraction-guidelines-for-in-vehicle-electronic-devices.

68. Ibid.

69. Juan Londoño, “How Extended Reality Tools Can Improve Training for First Responders” (ITIF, June 17, 2022, https://itif.org/publications/2022/06/17/extended-reality-tools-can-improve-training-for-first-responders/.