Reality Check:

How to Protect Human Rights in the 3D Immersive Web

MARIANA OLAIZOLA ROSENBLAT

NYU | STERN

Center for Business and Human Rights

September 2023

Contents

Author

Mariana Olaizola Rosenblat is a policy advisor on technology and law at the NYU Stern Center for Business and Human Rights.

Paul M. Barrett, the NYU Stern Center's deputy director, provided assistance with the conception and editing of this report.

Acknowledgments

We are grateful to Craig Newmark Philanthropies and the Open Society Foundations for their continued support of our work on technology and democracy.

Executive Summary

The "metaverse," "extended reality" (XR), and "spatial computing" are all terms that describe what is expected to become the next iteration of the Internet: a sprawling collection of online spaces and applications offering digital content to users in three-dimensional, immersive form.

> "This report examines two of the most pressing issues related to the mass adoption of immersive technologies: the potential erosion of privacy, including mental privacy, and the proliferation of harmful behavior in virtual environments, including sexual harassment and abuse of children."

Instead of interacting with digital content via two-dimensional images and text on flat screens, consumers will be able to carry out everyday activities—from schooling to work to shopping—in environments that feature 3D computer-rendered objects, places, and people.

The advent of XR platforms could be as important as the rise of the Internet in the 1990s in terms of its far-reaching, if uncertain, potential to transform daily life. Some claims about the 3D immersive web—what precisely it will look like, who will own it, how much economic value it will yield, and when it will mature—are largely speculative. But other aspects of the new medium are already discernible and raise urgent policy questions.

This report examines two of the most pressing issues related to the mass adoption of immersive technologies: First, there is the potential erosion of privacy, including mental privacy. XR devices and systems require the processing of users' bodily data and spatial surroundings. When aggregated and analyzed over time, this data can reveal highly sensitive information about individuals, including their physical and mental states—information that could be exploited for commercial or political gain. The second issue is the proliferation of harmful behavior in virtual environments, including sexual harassment and abuse of children. Experiences in virtual reality often are perceived by users as real and can result in deep and lasting psychological harm. Yet the tools and systems to ensure safety in XR are underdeveloped.

The report also briefly considers other potential hazards exacerbated by 3D immersive platforms. It concludes with pragmatic recommendations for the industry and policymakers to act proactively to protect human rights in the 3D immersive web.

Here are our recommendations, in capsule form, for how to manage the risks related to immersive technologies:

Recommendations to XR platforms

1. **Protect user body-based data by erasing it.** Given the sensitivity of body-based data collected and processed by XR systems, companies should commit to erasing all raw and derived bodily data as soon as it is no longer needed for device functionality.

2. **Provide various options for users to control their exposure to risk.** XR platforms should offer users various options to limit the type of data collected and processed by their devices and systems. They should also provide a variety of safety tools and settings for users to control their experience.

3. **Incorporate privacy, safety, and security best practices.** Companies should adopt known best practices on privacy, safety by design, and cybersecurity before launching their products.

4. **Invest in the development of 3D classifiers.** The real-time, ephemeral nature of interactions in XR makes it crucial for platforms to detect high-risk behavior, such as efforts at child exploitation and extremist recruitment, before it results in serious harm. Doing so at scale requires companies to invest in automated systems with 3D classifiers that can carry out proactive moderation in immersive virtual environments.

5. **Provide clear and accurate information to the public.** To earn the public's trust, XR platforms should provide clear, comprehensive, and accessible information to users about critical aspects of the technology that might affect their privacy, safety, and security.

6. **Include people with diverse abilities and lived experiences.** To avoid exacerbating digital divides and inequality, companies should include individuals of diverse abilities and backgrounds in their product design, development, and deployment teams.

Recommendations to Government

7. **Pass comprehensive federal privacy legislation.** Congress should pass a comprehensive privacy law that, in addition to safeguarding other aspects of consumer privacy, restricts the use of body-based data for profiling users and strengthens the concept of user consent.

8. **Strengthen federal authority and capacity to oversee digital industries.** Congress should reinforce the Federal Trade Commission's mandate to protect consumers against unfair and deceptive practices by technology companies, including XR platforms. Alternatively, Congress should create a new, specialized federal body tasked with this mandate.

9. **Invest in research.** The government should empower federal agencies to investigate the health consequences and environmental impact of XR immersive technologies.

1. Introduction

Over three decades ago, author Neal Stephenson described a future in which humans could enter a virtual, or computer-simulated, world and interact within it as digital personas, or avatars. His highly influential 1992 novel, *Snow Crash*, called this parallel virtual world "Metaverse."

> "Inhabiting computer-simulated environments that mimic and blend with real life is no longer the exclusive province of science fiction. It is already possible."

The novel depicts a time when private corporations have largely displaced governments and shady moguls exercise control over chunks of the world's territory. A malevolent media magnate named L. Bob Rife tries to infect people's brains with a digital drug (or virus) in order to manipulate them for his benefit. Hiro Protagonist, a savvy programmer, and his allies navigate the Metaverse in search of clues that will help them thwart Rife's scheme, eventually finding an effective anti-virus and saving humanity.[1]

Apart from its dystopian plot, Stephenson's work was prescient in depicting features of virtual reality—avatars, virtual real estate, and digital economies—that contemporary real-life tech entrepreneurs aim to build. In 2023, the advent of a densely-populated virtual universe that hosts much of human activity is still a long-term ambition. But technologies that are already on the market and becoming increasingly accessible point toward a realistic near-term future in which 3D immersive interaction with digital content starts to eclipse the 2D Internet.

Inhabiting computer-simulated environments that mimic and blend with real life is no longer the exclusive province of science fiction. It is already possible. The technologies that enable aspects of such experiences have been available to consumers for years. These include virtual reality headsets, smart glasses, and other wearable devices that infuse a user's physical environment with computer-generated sights, sounds, and other sensory stimuli.

Thus far, these gadgets have remained outlier technologies due to steep prices, issues with comfort, and the lack of sufficiently appealing content to compensate for such shortcomings. But the technologies are advancing steadily and approaching a threshold of sophistication and affordability that will make them ripe for mainstream consumer use. Meta, which changed its name from Facebook in 2021 to mark its pivot from 2D social media to the metaverse, has already plowed more than $40 billion into Reality Labs, the company unit developing virtual-reality products.[2] Other tech giants—including Microsoft, Google, Nvidia, and Sony—also have made sizable investments in XR.[3]

And in June 2023, Apple announced the upcoming release of its Vision Pro headsets, reigniting popular interest in the projection of digital objects spatially in one's physical surroundings.[4]

Millions of people are already familiar with 3D virtual worlds created for online games. Platforms traditionally dedicated to online gaming have realized the potential of 3D immersion and branched out to other forms of entertainment, socializing, and commerce. Epic Games, the publisher of the popular multiplayer videogame *Fortnite*, has used its platform to host real-time virtual concerts featuring celebrities like Ariana Grande and Travis Scott. Roblox, a game-creation platform, is home to virtual commercial establishments, including "Nikeland," which sells Nike fashion for avatars.[5]

Much of the discussion around immersive technology—also referred to as extended reality (XR), spatial computing, or the metaverse—focuses on its impressive potential applications: doctors rehearsing open-heart surgeries on virtual patients or students exploring the pyramids of Giza merely by donning headsets. But these technologies also have the potential for far-reaching harm to human rights, particularly the rights to privacy, autonomy, and safety. This report assesses the foreseeable risks that accompany the move from 2D to 3D digital spaces and makes pragmatic recommendations to mitigate them. In particular, the report focuses on what the private sector driving this technology should do proactively to prevent significant harm.

The report also highlights the importance of timely policy deliberation and action in this area. Technological developments, such as the advent of social media and the more recent introduction of generative artificial intelligence, have left many policymakers scrambling to understand their effects on society even as the technologies continue to advance and unleash societal-scale consequences. In the case of immersive technology, which has yet to reach mass-market adoption, policymakers have the luxury of *some* time to consider the risks that are in store and put in place measures to manage them. But we should not delay—an immersive 3D web is coming, and we should prepare for it.

Various Realities:
Several Types of 3D Immersion

- **Virtual reality (VR)**
  Full immersion in a computer-simulated environment. Today's VR relies on head-mounted displays to render images and spatial (3D) audio, and haptic wearables like vests and gloves to provide tactile feedback.
- **Augmented reality (AR)**
  The physical, real-world environment overlaid with digital content. Today's AR devices include mobile phones (for AR applications like Pokémon Go) and AR headsets or smart glasses.
- **Mixed reality (MR)**
  A more advanced version of AR that allows users to manipulate and interact with digital objects as if they were real.
- **Extended reality (XR)**
  An umbrella term for all forms of computer-altered reality, including VR, AR, and MR.

“Much of the discussion around immersive technology focuses on its impressive potential applications. But these technologies also have the potential for far-reaching harm to human rights, particularly the rights to privacy, autonomy, and safety.”

2. Heading Into an Immersive Future

Visions of the 3D virtual future vary. Some futurists, like Matthew Ball, envision a unified system of interconnected 3D worlds, similar in scale and interoperability to the current Internet.[6] But its realization along these lines is far from guaranteed given the competitive interests of technology companies.[7] Instead, today's tech giants—Meta, Google, Apple, and Microsoft—may well come to own and operate large chunks of the metaverse as mostly closed ecosystems, or "walled gardens."[8]

> **"Despite a dip in venture capital investment in 2023, major technology companies continue to pour billions of dollars into immersive technologies, signaling their intention to retain their dominance in the transition from the 2D to the 3D web."**

The precise features and business models of the metaverse are under development and will likely change over time. This report considers the metaverse in general terms, as a collection of online spaces offering digital content and experiences to users in a spatial fashion—that is, as part of their natural surroundings.[9] Several such platforms already exist, catering principally to gamers.

VRChat, an online virtual-world platform, consists of thousands of interconnected 3D worlds where players interact through user-created avatars. Meta's Horizon Worlds is a similar platform, offering 3D immersive events, games, and social activities—some hosted by Meta and others created and managed by independent developers. The game-creation platform, Roblox, which has wide appeal among children, is available in VR mode and continues to expand its compatibility with various headsets.[10]

Despite ardent following among some technology enthusiasts and gamers, the metaverse has lately fallen out of fashion among Silicon Valley pundits. Meta's flagship virtual platform, on which it has invested aggressively since the company's rebranding in 2021, has met with lackluster reception from users and tech analysts.[11] The company's Reality Labs unit has lost more than $21 billion since the beginning of 2022, prompting Meta to trim the department's headcount and align itself with the hype surrounding generative artificial intelligence.[12] But despite a dip in venture capital investment in 2023,[13] major technology companies continue to pour billions of dollars into immersive technologies, signaling their intention to retain their dominance in the transition from the 2D to the 3D web. Ongoing investments by Big Tech and governments around the world[14] have led consultancies and financial institutions to make bold projections of the metaverse's value in 2030, ranging from roughly $1 trillion to nearly $22 trillion.[15]

Companies investing in XR rely on a variety of business models. On one end of the spectrum are companies that offer "free" content and services in exchange for user data, which they monetize by creating consumer profiles for targeted advertising. Meta and Google's business models largely rely on ad sales. On the other side of the spectrum are companies, like Microsoft, that tend to charge subscriptions for content and services. In the middle are platforms that operate under taxation models, taking a percentage cut from content creators' profits and other in-platform transactions. Epic Games and Roblox fall into this category.[16] Other ways to make money in the XR space include sales of hardware, such as Apple's high-end Vision Pro, and the issuance of proprietary digital currencies that support user-based economies in decentralized platforms like Decentraland.[17]

Promising applications

It is worth identifying some promising uses for immersive technologies before moving on to the likely hazards.

According to Jeremy Bailenson, the director of Stanford's Virtual Human Interaction Lab, "training is the home run of VR," especially for situations in which training is otherwise costly, impractical, or dangerous.[18] VR applications have been used to train military officers, airplane pilots, oil field workers, surgeons, emergency medical technicians, and firefighters.[19] They enable realistic experiential learning while minimizing risks, time, and costs.

In addition to workforce training, immersive VR simulations have proven effective in bias-training, which works by immersing users in the experiences of people of diverse races, abilities, and backgrounds to enhance their understanding and empathy.[20] For example, in the powerful simulation "Carne y Arena" by Alejandro G. Iñárritu, users embody migrants as they undertake the perilous journey across the US-Mexico border.[21]

The benefits of immersive hands-on learning may also be brought to the classroom, where abstract instruction can be supplemented with realistic 3D visualizations and experiences. Schools have explored taking students on virtual field trips to historical sites, outer space, and even the inner biological systems of living organisms.[22]

Immersive technology has also been touted as the next frontier in the realm of healthcare, where it has been applied to develop therapies for post-traumatic stress disorder (PTSD), claustrophobia, and social anxiety.[23] Additionally, products like NeuroRehab VR leverage movement-tracking technology to optimize treatments for patients with orthopedic and neurological conditions, including stroke survivors.[24]

The most common applications of XR technology today are in the realms of entertainment and socializing. Users

How It Works:

Core Technologies Underpinning the Metaverse

- **Hardware devices**, including head-mounted displays, sensors, haptic wearables (meaning those allowing for a sense of touch), and brain-computer interfaces, enable a spectrum of 3D immersive experiences.
  - VR headsets are used for 3D immersion in fully digitally rendered environments. *Example: Meta's Quest Pro*.
  - Haptic controllers, full-body suits, and other wearables provide tactile feedback. *Example: Immerzs' KOR-FX haptic vest*.
  - AR headsets and smart glasses embellish the real world with virtual content. *Example: Snapchat's Spectacles*.
  - Neural interfaces, also known as brain-computer interfaces, are largely experimental devices that translate brain signals into digital commands in real time. *Example: Neuralink's implant*.
- **Artificial intelligence systems** enable sophisticated data processing, faster 3D content creation, advanced avatar animation, the population of virtual worlds with computer-controlled avatars, and automated content moderation.[1]
- **Blockchain technology** provides the building blocks for decentralized platforms and digital economies, believed to be key to a decentralized and interoperable metaverse.

[1] https://www.xrtoday.com/mixed-reality/what-is-the-metaverse/; https://www.forbes.com/sites/bernardmarr/2023/05/23/digital-twins-generative-ai-and-the-metaverse/?sh=1dc087a57362

of social VR platforms, such as VRChat, enjoy being embodied in avatars whose appearance they have chosen and customized. The platforms also provide viable means to form communities and feel physically present with people even when they are hundreds of miles away.[25]

But some exploratory uses of immersive platforms are premature and misguided. In countries like Colombia and China, judges have held legal proceedings in the metaverse, reasoning that virtual court appearances can make for more realistic interactions than regular video conference calls. However, as legal and XR experts Daniel Castano and Brittan Heller caution, this use of the metaverse is ill-advised.[26] Contrived avatar animation capabilities and other functional limitations of XR technologies have the potential to distort impressions of defendants and witnesses, leading to skewed and unfounded assessments of credibility. Moreover, XR hardware with good-quality image rendering is expensive and lacks adequate accessibility features, introducing additional inequities into judicial processes.

Beneficial uses of immersive technologies exist, but the considerable risks posed by these technologies weigh in favor of exercising caution before deploying them. In particular, the technologies pose serious risks for privacy and safety—risks that must be managed carefully to prevent wide-ranging and potentially irreversible harm.

Leading Competitors:

A Selection of XR Industry Players

Hardware platforms

Meta Quest

Meta's Quest and Quest Pro

Vision Pro

Apple's Vision Pro (forthcoming)

VIVE

HTC's Vive

Microsoft HoloLens

Microsoft's HoloLens

Software platforms

horizon

Meta's Horizon Worlds and Horizon Workrooms

STEAM VR™

Steam VR

Decentraland

Decentraland

Developer Engines

UNREAL ENGINE

Epic's Unreal Engine

Unity

Unity's XR Interaction Toolkit

NVIDIA OMNIVERSE

Nvidia's Omniverse

3. What Could Go Wrong

In the era of Internet search engines and social media, many people have grown accustomed to having their online communication and behavior tracked to some extent. The business models built around targeted advertising, feeding a system that Shoshana Zuboff aptly called "surveillance capitalism," has made Silicon Valley one of the most profitable industries in history.[27] This business model is now a known and accepted, if still controversial, part of contemporary life.

> "The types and volumes of data that XR devices can collect make them several orders of magnitude more invasive than traditional web-tracking and surveillance technologies."

Against this backdrop, a new technology's incursion into privacy may strike some readers as inconsequential. But this perspective fails to account for the unprecedented nature of the data collection capabilities of XR technologies.

Privacy is recognized as a human right for a reason.[28] Liberal democracy is rooted in the assumption that individuals are entitled to a personal sphere exempt from state (and corporate) interference. Without this sphere, individuals cannot freely explore and develop their identity and convictions.[29] We carry on daily life assuming that no one has access to our innermost thoughts, medical conditions, sexual preferences, and emotional vulnerabilities. The possession of such information would amount to an inordinate amount of power to extort, manipulate, and coerce.

XR technologies are designed to collect and process precisely such intimate personal information. In fact, XR technologies cannot function adequately without collecting and processing large quantities and various types of personal data—specifically, bodily data that can also be used to infer behavioral and psychological information about individuals.[30]

Conventional XR hardware is equipped with sensors that continuously track at least three types of user data: head movements, eye movements, and spatial maps of physical surroundings. Head-position and movement tracking are needed to calibrate headsets and prevent motion sickness during an immersive experience. Eye movements, captured by inward facing cameras on headsets, allow users to interact with virtual content based on where they direct their gaze. Without eye-movement tracking, the computer image generator would not respond to users' change in focus or attention, severely limiting the immersive nature of the experience. Eye-movement tracking also enables avatars to simulate eye contact. Spatial maps of users' physical surroundings, captured by outward-facing cameras on headsets, position the user in relation to digital content and help to prevent accidents, such as running into physical objects during an immersive experience.[31]

Advanced hardware can track additional bodily data for even more realistic 3D immersion and virtual interaction. This includes facial expressions for avatar animation, hand and other limb movement for full-body immersion and multi-user interaction, pupil dilation data to render crisper visuals, iris or retina images for user authentication, and voice data to enable oral interactions and commands.[32] Depending on the immersive experience, a user may also consent to other types of physiological tracking, such as their heart rate, respiration, and blood pressure. Such tracking may be desirable in certain fitness, wellness, and medical applications.

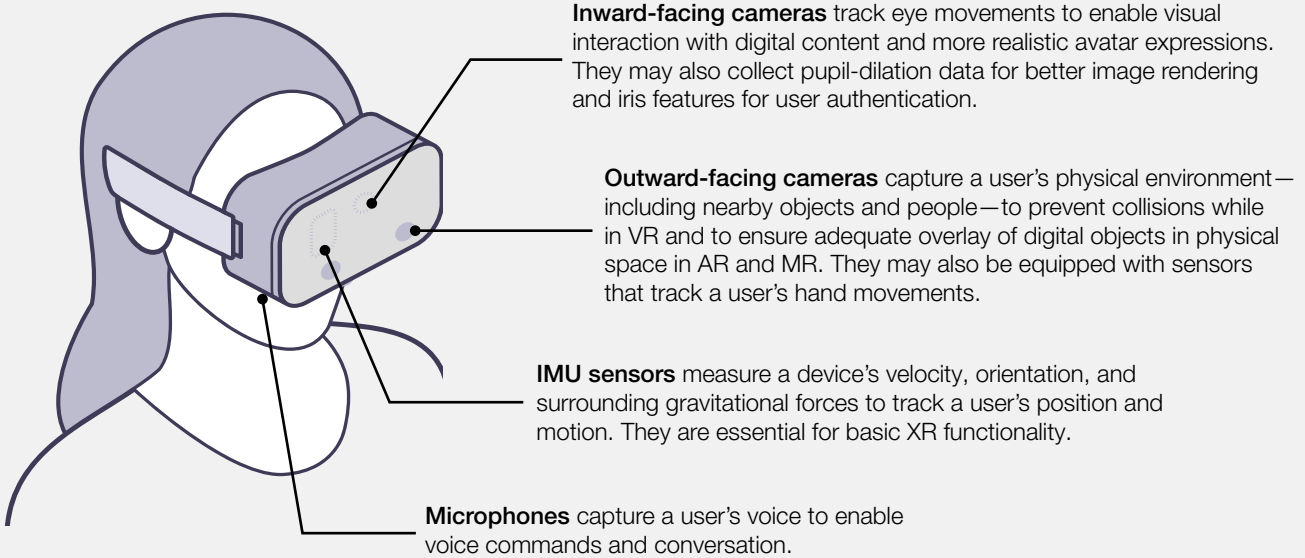
The types and volumes of data that XR devices can collect make them several orders of magnitude more invasive than traditional web-tracking and surveillance technologies.[33] When analyzed over time, they reveal an individual's involuntary and immutable characteristics, including their vocal inflections, gait patterns, detailed facial expressions and gestures, movement idiosyncrasies, and real-time physical responses to stimuli. What makes these emerging technologies most problematic is not the mere capture and processing of such data, but how the collected data could be aggregated and exploited.

Scientists at the University of California at Berkeley and the company Unanimous AI have shown that even the most basic motion tracking required for XR functionality can be used to derive information about the identity, demographic characteristics, and even health of a user. Their 2023 study confirmed that motion data "is a biometric that belongs in the same category as blood type or an iris scan."[34] Applying a machine learning model to the movements of 55,000 known users playing the popular VR game Beat Saber, the scientists were then able to discern the identity of each user with 94% accuracy from just 100 seconds of basic body motion data. Even more troubling than its biometric capabilities, the motion data could be used to infer over 40 behavioral attributes of each user, including specific mental and physical conditions.[35]

These findings with respect to motion data are worrisome enough. But when XR systems are given access to other bodily data—like heart rate, blood pressure, perspiration rate, pupil dilation, and brain signals—they enable even more sophisticated analysis of users' physical, emotional, and mental states.[36] Such information could be used to derive "biometric psychography," profiles of individuals' interests, aversions, and vulnerabilities based on their involuntary and often unconscious reactions to stimuli. In effect, this type

Sensors and Data Streams:

How XR Devices Extract Body-Based Data



Meta versus Apple:

Implications for User Data

Meta and Apple—two of the largest competitors in XR—are known to take divergent approaches to user data. Meta harvests user data to create consumer profiles for targeted advertisements. Apple makes most of its revenue by selling expensive hardware and charging steep commissions on apps and in-app purchases on its App Store. Apple's business model allows it to present itself as a credible guardian of privacy. By contrast, Meta's claim to prioritize privacy[1] may seem questionable to some people, given its longstanding ad-based business model.

Meta's terms of service and privacy policies applicable to its metaverse products leave the door open for the company's continued monetization of user data collected by the devices. Once users turn on eye tracking, hand tracking, audio, and facial-expression tracking to enhance their immersive experience, their data is subject to wide-ranging use by the company.[2] Meta disclaims responsibility for the data practices of third-party developers with whom the company shares user data.[3]

In an attempt to downplay the risk of this liberal data-sharing approach, Meta emphasizes that it shares only "abstracted," rather than "raw," body-tracking data. Yet, as a former Meta Reality Labs employee noted in an interview, "abstracted [eye-gaze] data reveals where your attention is going and allows for the extrapolation of patterns, which could potentially be very sensitive information."[4]

In contrast to Meta, Apple has vowed not to collect any eye-movement data, whether raw or abstracted. This commitment deserves commendation. However, it is important to note what Apple has *not* mentioned—namely, what it will do with body-motion and face-tracking data. The company has yet to release its detailed privacy policy for the Vision Pro, which is expected to go on sale in early 2024. But if the company plans to make available any multi-user 3D immersive experiences through its new spatial computing platform, it will have to contend with how to protect sensitive motion data from misuse by third parties.[5] Apple declined to comment.

[1] https://about.meta.com/metaverse/responsible-innovation/

[2] Meta gives itself wide latitude to use customer data to improve its products and "to send personalized commercial content." https://www.meta.com/legal/privacy-policy/.

[3] https://www.meta.com/legal/privacy-policy/. The company says: "Please note that information you share with these (or other) third-party services will be subject to their own terms and privacy policies, not this policy." Meta states that developers should refrain from certain uses of data shared with them. However, Meta does not audit third parties' actual data handling practices and simply requires them to self-certify their compliance with the policy. https://developer.oculus.com/policy/data-use/.

[4] Interview with former company employee, on file with author.

[5] Interview with XR expert, on file with author. For some potential and planned user experiences on the Vision Pro, see https://www.theinformation.com/articles/what-apple-didnt-reveal-about-the-vision-pro?utm_term=popular-articles&utm_campaign=article_email&utm_content=article-10737&utm_source=sg&utm_medium=email&rc=tltwje

of data enables a form of mind reading—the continuous recording of what "users are looking at, how long their attention is captured, and how users may feel about what they are seeing."[37]

Although body-based data need not be used for purposes other than device functionality, the ability to use or sell such information may be too tempting for some. As Avi Bar-Zeev, an XR expert and advisor to technology companies, noted at a recent conference, "companies are salivating at the prospect" of monetizing the troves of sensitive data that XR devices can collect.[38] This data, in turn, could be used to build models that act as powerful influence machines calibrated to achieve commercial, political, and other ulterior ends.

Louis Rosenberg, an XR expert and founder of Unanimous AI, makes a compelling case that such systems are within reach. In a recent paper, he explains how the metaverse might become "the most dangerous tool of persuasion ever created" by pairing real-time surveillance with real-time influence. Essentially, "large and powerful metaverse platforms could track billions of people and impart influence on select individuals by altering the world around them in targeted and adaptive ways."[39] Such influence could easily slip into insidious manipulation, whereby users' involuntary reactions to stimuli get fed into a system that curates their digital content and experience in a way that optimizes for specific responses—for example, their decision to purchase a particular product or inclination to believe certain disinformation.[40]

Adding generative artificial intelligence into the mix could further darken the picture. Generative AI tools built from large language models, which today are used to power text-based conversational apps like ChatGPT, could soon be programmed into avatars in the metaverse. These embodied AI agents,

what Rosenberg calls "Virtual Spokespeople," would be indistinguishable from actual humans absent disclosure mandates.[41] Moreover, they could be armed with a wealth of real-time data about the objects of their influence, enabling super-targeted influence operations at scale. Without adequate safeguards, such systems could be deployed by corporate actors to maximize profits, as well as by government and non-state actors to advance their political agendas.[42]

There are other dangerous potential uses of data captured by XR devices. The outward-facing cameras on XR headsets that track users' physical surroundings can have serious collateral consequences on the privacy of non-users of the technology. AR devices are of particular concern because they are designed for prolonged use in people's natural surroundings. Their "always-on" scanning has the potential to capture the gait patterns, facial expressions, and eye movements of bystanders, who have not given their consent.[43] Furthermore, headsets are equipped to constantly scan physical objects for spatial cues. When used en masse, such perpetual scanning of the world and its inhabitants could enable constant surveillance of public and semi-public places.[44]

Unfortunately, existing laws in the United States and in most parts of the world contain loopholes that make these dystopian futures all too possible. The U.S. lacks a comprehensive federal privacy law, and the privacy laws that exist at the state level fail to protect consumers against many types of dangerous data gathering and uses enabled by XR systems.[45] Most state laws protect a type of data known as "personal identifying information," or PII,[46] and a few focus on protecting biometric information, defined as data that can be used to identify a unique individual.[47] By protecting narrowly defined categories of "sensitive" or biometric data, rather than regulating harmful uses of all personal and body-based data, these laws leave the door open for companies and other actors to harvest data to create profiles of consumers for targeted advertising, political influence, and other manipulative purposes.[48]

In the U.S., only California has a law that potentially protects consumers against profiling not necessarily tied to identification—but only in some cases. The California Consumer Privacy Act protects personal information when it is used "to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."[49] The law gives California residents the right to opt out of the *sale* or *sharing* of such data, but not its collection or use by the entity doing the collection.[50] It does not set limits on what first-party collectors themselves can do with the data, as long as the collector provides notice to consumers.[51] Moreover, the law adopts a narrow definition of "business"[52] that potentially leaves out many content developers and small platforms that are likely to handle user data in XR.

Outside the U.S., the European Union's General Data Protection Regulation (GDPR) contains the most robust protections of consumers' data. The law applies to any type of personal data that is "used for learning or making decisions about an individual" and which "could have an impact on [that] individual."[53] The GDPR also bans the processing of certain categories of sensitive personal data,[54] unless the individual provides explicit consent. But therein lies the catch: nearly all legal protections of personal data—in Europe, the U.S., and elsewhere—disappear if a consumer consents.

Privacy regimes that rely on notice and consent as the primary mechanism of privacy protection have proven ineffective because companies are skilled at coaxing users into agreeing to their terms of use.[55] In the U.S., this notice-and-consent paradigm, enshrined in most privacy laws, has failed to protect individuals' actual privacy interests.[56] Online services comply with privacy laws by drowning users in lengthy and legalistic consent agreements, which consumers tend to readily accept without understanding their implications.[57] The GDPR's consent rules are more stringent, requiring that terms be "intelligible and easily accessible."[58] However, again, many users agree to the terms, if only because doing otherwise deprives them of the ability to use a desired product or service.[59]

A final limitation of the legal protections in place is that they leave most of the world's population without a say on how technology companies use their data. Immersive platforms are borderless, but regulation is jurisdictional.[60] The GDPR primarily protects residents of the E.U. In the U.S., some states lack any type of legislation on data privacy, leaving their residents at the mercy of companies and data brokers.

But the XR industry need not wait for regulation to act responsibly. Companies can voluntarily adopt best practices on data protection and use to provide their customers with a strong first line of defense against illegitimate practices that violate the rights to privacy and autonomy. These best practices are mentioned in the recommendations section of this report.

Physical aggression and lawless virtual spaces

To someone who has never experienced VR immersion, saying that a person suffered physical assault in the metaverse may seem like an exaggeration.[61] Can we really call it *physical* assault when talking about cartoonish avatars interacting in a computer-simulated environment? According to psychologists, the answer is yes.

Mel Slater, a professor at the University of Barcelona and co-director of the EVENT (Experimental Virtual Environments for Neuroscience and Technology) Lab, uses the term "psychological realism" to explain why people immersed in an XR world have the sensation that what they are experiencing is real.[62] Numerous studies show that people "respond realistically in virtual environments, even when they know with certainty that nothing real is happening."[63] A related phenomenon, which Slater calls "virtual embodiment," describes how people readily adopt virtual bodies as their own. In effect, they process any aggression inflicted on the fake body as real sensory experiences.[64] With increasing refinement of immersive affordances (more realistic graphics, full-body avatar animation, haptic feedback, etc.), the perception of reality and embodiment become more pronounced.[65]

Psychological realism and virtual embodiment are what make virtual reality compelling. Virtual exposure therapy would not work effectively if patients did not have a strong sense of actually being exposed to the objects of their phobias. VR skydiving and roller coasters would not be so thrilling without the brain flooding the body with adrenaline during the virtual experience. But this perceptual realism also makes virtual reality more dangerous. Slater offers the example of a person instinctively trying to sit in a virtual chair that has no counterpart in reality and falling to the floor, harming themselves.[66] Solo VR experiences can certainly pose risks of this sort. But the potential for harm escalates in multi-user environments, where the author of the VR environment cedes control over much of the experience to other people, some of whom may be inclined to cause havoc.

Many online spaces are plagued with interpersonal abuse, including sexual harassment, bullying, mobbing, stalking, and child sexual grooming.[67] The same behaviors have been observed in social VR environments with alarming prevalence.[68] Like in many online spaces, users of social VR tend to feel emboldened by the anonymity of their virtual personas and their presumed detachment from reality.[69] Chanelle Siggens, a *New York Times* reporter, recounts an incident in which a male avatar groped her in a VR game. She asked the person to stop, and he "shrugged as if to say: 'I don't know what to tell you. It's the metaverse – I will do what I want.'"[70]

But harassment in VR can leave or aggravate deep psychological scars.[71] According to Michelle Cortese, a VR designer and adjunct professor at NYU, the "visceral quality of VR abuse can be especially triggering for survivors of violent physical assault." She spoke from personal experience:

"[T]here I was, surrounded by friends in real life, punching virtual goons in VR, when it happened: a large [non-player character] got way too close, loomed over me, pushing and gesticulating… and I panicked. I innately sensed a familiar knee-jerk reaction to an incoming assault. My heart sank… My body responded to virtual stimuli with real-life survivalism."[72]

The experience of being re-traumatized in VR motivated Cortese to help the Social VR department at Meta—where she worked—take safety in VR more seriously. Meta's Social VR department would later develop and release Meta Horizon Worlds. With her colleague, Andrea Zeller, Cortese proposed a series of design approaches based on real-world consent paradigms that gave rise to personal safety bubbles.[73] A personal safety bubble—or "personal boundary" as it is referred to in Horizon Worlds—is a variably sized buffer that surrounds a user to protect them from unwanted contact from other avatars. Meta originally did not prioritize the personal boundary feature for the public release of Horizon Worlds but added the feature in February 2022 following accounts of virtual harassment. The company now highlights the feature when questioned about safety in VR.[74]

Since its 2017 launch of Facebook Spaces, the company's first VR product, Meta has taken steps to improve safety in virtual reality. Aside from offering the Personal Boundary feature, the company has implemented a Pause button that enables users facing aggression to escape into a space where no one can touch or interact with them. While in Pause, users can mute, block, and report an aggressor.[75] The company pointed out to us that it has developed other tools to give users additional control over their experiences, including a Voice Mode feature that "garbles" the voices of certain users, and options to blur text chats from strangers and filter out words that might be upsetting or offensive.[76]

The company also decided to prioritize safety when it announced that every Meta headset would record users' most recent interactions in Horizon Worlds to enable user reporting of illegal or harmful activity. According to Meta, these recordings are processed on users' devices and promptly deleted unless a user sends them to the company as supporting evidence of a conduct violation. The company says it uses the recordings only to resolve those user reports and promptly deletes them from its servers, which is a wise decision from the standpoint of user privacy.[77] Meta also says it employs an unspecified number of Horizon World "safety specialists" to intervene and document conduct violations in real time.[78]

Yet Meta has set a limit on how much it is prepared to ensure user safety in apps and experiences developed by third parties and sold on its platform. In May 2023, the company announced that user reports of safety violations in third-party apps listed on its platform would have to be handled by developers

directly.[79] Aside from notifying app developers that they were responsible for reviewing and resolving such reports, Meta did not commit to taking proactive steps to ensure that such reviews would actually occur. However, when asked about this issue, the company noted: "Users who experience governance issues with an app can notify us via the Flag This App button on every app's Product Details Page. We use feedback from this and other sources, as well as our own research and testing, to conduct app assessments. Where there is a persistent and egregious failure to meet reporting and governance requirements, we take enforcement action, such as adding warning labels to the Product Details Page or removal from the Quest Store."

Meta could improve its approach to safety in other respects. Despite recent updates, the company's Code of Conduct for Virtual Experiences remains ambiguous and under-inclusive. For example, the company could provide a better explanation of the distinction between "public" and "closed" spaces and its implication for moderation and users' expectations of privacy.[80] It is unclear whether Meta monitors closed spaces—which it analogizes to "your own living room"—for illegal or egregious behavior like child exploitation or extremist recruitment that is unlikely to be reported by the individuals involved. Given the higher stakes of abuse in immersive environments, Meta should set clearer and higher expectations of conduct on its VR platform that at least match Facebook's Community Standards in terms of their detail and comprehensiveness.[81] It should also explain how it strives to fulfill those expectations. Doing so would help improve conduct norms in VR, which are malleable, but tilting toward lawlessness and toxicity in some cases.[82]

Andrea Zeller and Michelle Cortese, former VR designers at Horizon Worlds, suggest that XR platforms generally could instill and enforce conduct norms more effectively. Rather than presenting rules and expectations in 2D texts that few users read and internalize, platforms and content developers could leverage the immersive nature of the medium to demonstrate conduct norms and safety features dynamically during onboarding and at other timely moments.[83]

Additionally, platforms and developers could reward positive behaviors and discourage anti-social ones, drawing on design strategies that have proven useful in the gaming context.[84] They could appeal to players' desire to be recognized as valuable participants in a virtual community by, for example, awarding badges and special titles to those with a good track record of displaying sportsmanship and mentoring others.[85] They could also use platform "community guides"[86] and non-player characters (NPCs) to model positive behaviors.[87] These norm-setting initiatives could prevent problematic cultures from taking hold.[88]

Besides shaping community norms, a clear and engaging introduction to rules and expectations would allow XR users to decide whether to join a particular experience and, if so, whether to activate preemptive safety controls. Cortese emphasizes the importance of what she calls "experience curation" as a partial solution to user safety. In effect, companies can empower users to take control of their own safety in XR. But to do so, platforms must provide accurate and timely information about what an experience entails—through, for example, onboarding simulations and informative safety ratings—and also offer customizable and intuitive self-help tools that users can easily deploy when faced with a real-time threat.[89]

Beyond adopting safety-by-design strategies, XR platforms need to develop proactive and reactive

> **"Harassment in VR can leave or aggravate psychological scars."**

moderation systems. Given the real-time, ephemeral nature of interactions in VR, proactive detection is the only way to catch and address certain dangerous activities like child sexual exploitation and terrorist recruitment before they cause irreparable harm. But, according to Brittan Heller, the potential for proactive moderation in XR is severely limited by the lack of curated datasets of 3D content needed to train AI models—known as 3D classifiers —to carry out moderation.[90] Without such classifiers, XR companies largely rely on users to flag illegal and other harmful activity and a small number of human reviewers to address those reports retroactively. This approach is insufficient to ensure safety across the millions of interactions and experiences happening simultaneously in VR, and it underscores the need for companies to invest in developing automated moderation systems that can detect harmful behavior in 3D environments.

Children's exposure to abuse

In 2022, researchers for the Centre for Countering Digital Hate (CCDH) set out to study social experiences in VRChat within Meta's Horizon platform. They documented the frequency of graphical sexual content, racist harassment and bullying, threats of violence, and child sexual grooming, finding that users in VRChat were "exposed to abusive behavior every seven minutes."[91]

Preventing Extremism in VR:

Two Contrasting Approaches

If online gaming provides any lessons for the VR space, it is that bad actors will try to exploit immersive environments to spread hateful, violent, and extremist narratives.[1] Content and behavioral moderation in gaming spaces has lagged behind mainstream social media.[2] One reason for this is the lack of human capacity and technical tools to do moderation in real time and at scale. Another reason is companies' reluctance to moderate gaming chatrooms, either because of financial considerations (content moderation is expensive and difficult to do well) or a libertarian ethos that justifies turning a blind eye to harmful activity, or both.

VR platforms face the same challenge on moderation. These platforms provide spaces for real-time virtual interactions among largely anonymous users in fully immersive 3D environments, but they lack the human and technical capacity to ensure that those interactions do not result in significant harm. While there is no solution that would eradicate all online harm, there is room for platforms to take more responsible approaches, especially in how they vet the VR experiences they sell. Valve and Epic Games, two companies that offer VR experiences in their online game stores, provide a point of contrast.

Valve is notoriously libertarian when it comes to moderating and curating content. The company's official policy for its Steam platform, which offers thousands of self-contained VR spaces, in addition to traditional video games, is that it allows any type of content as long as it is not "illegal, or straight-up trolling." The company offers no details on how it understands these categories or how it enforces this ambiguous policy.[3]

Epic Games, which declined to comment for this report, seems to take a different approach. Its content guidelines for games and VR experiences sold in its Epic Games Store prohibit content that is hateful or abusive, which includes "content that promotes hatred, abuse, racism, or discrimination against groups or individuals" and "content that promotes terrorist or extremist organizations." The company does not elaborate on how it enforces this policy, however.[4]

[1] Suraj Lakhani, When the Physical and Digital Combine: The Metaverse and Gamification of Violent Extremism, Perspectives on Terrorism, Vo. XVII, No. 2, June 2023.

[2] https://bhr.stern.nyu.edu/tech-gaming-report

[3] https://steamcommunity.com/games/593110/announcements/detail/1666776116200553082

[4] https://dev.epicgames.com/docs/epic-games-store/requirements-guidelines/content-ratings/content-guidelines

The researchers encountered older users indoctrinating younger ones in racist and homophobic ideas.[92] In one instance, an adult avatar rambled about the danger of mixing races and cultures, alluding to a supposed conspiracy of "white genocide."[93] In a virtual courtroom, a young girl with a black avatar was told by an adult player, "you're black, you're sentenced to death." Sexually explicit insults were also common. One adult repeatedly shouted lewd comments at a group of young girls and persisted in his aggression even after the girls said they were minors.[94]

At the time of the study, the app was listed in Meta's Oculus Quest Store as appropriate for children 13 and older, the same age limit the company applies to the use of its headsets. But in June 2023, Meta announced that it planned to lower the recommended age for the headsets, opening the door for children as young as 10 to enter its metaverse platforms.[95] When asked to explain this decision in light of reports of child abuse in some apps, Meta stated that "there's a vast array of engaging and educational apps, games, and more across our platform, the majority of which are rated for ages 10 and up by both the Entertainment Software Ratings Board (ESRB) and the International Age Rating Coalition (IARC)." The company also noted that it had set up parental controls to ensure that preteens receive their parents' consent before opening a Quest account and to help Meta recommend age-appropriate content.

Meta chief technology officer Andrew Bosworth wrote in an internal memo to employees that he aims for Meta's virtual worlds to have "almost Disney levels of safety." Yet in the same breath, he admitted that third-party developers would not be held to that high standard, and that policing how users speak and behave "at any meaningful scale is practically impossible."[96]

Meta could take could take a more responsible approach by regularly auditing the experiences that it makes available to children through its Oculus Quest Store and ensuring that user reports of harassment are adequately addressed. Meta's VR community forums contain at least several posts by parents expressing concern about their children's encounters with racism and bullying. In one post from February 2023, a parent voiced alarm that their "son was threatened and harassed violently on [G]orilla [T]ag," a VR game, and "worried about how this may affect him emotionally and physically." The parent implored the company "to have this properly taken care of."[97] In response to the post, and similar concerns expressed by other parents, a Meta community manager replied that the way to address the situation was "to contact the developers and make a report [sic] via their discord [server]." But, following its new user reporting policy for developers, the company provided no assurance to the parents that such a report would be received and resolved.

Aside from its technical limitations, the deployment of proactive moderation in VR may be controversial in some quarters. Real-time content moderation could be seen as treading too close to privacy-invasive surveillance systems. But the potential dangers of enabling harmful clandestine activities in unmoderated VR spaces justifies a bolder approach to safety, especially at this early stage in the technology's deployment. To set realistic user expectations of privacy, companies should explicitly inform users that their behavior in VR environments is subject to platform monitoring and moderation.[98]

Some form of age assurance may also be necessary to protect children from certain high-risk content, experiences, and interactions in XR.[99] Although privacy advocates may balk at the suggestion of recommending age assurance, they ought to consider that XR systems already collect massive amounts of data for basic device functionality, from which they could infer a user's age and channel it for more legitimate safety-enhancing purposes.[100]

The balance between safety and privacy can be a delicate one.[101] Fortunately, human rights law provides a useful framework for resolving tensions among fundamental human rights and interests. The framework consists of principles that can be applied by companies using a three-part test:[102]

1. Principle of Legality or Notice: Has the company provided clear notice to users about how communications and data are collected, monitored, processed, accessed, or otherwise used?

2. Principle of Legitimate Purpose: Does the collection, monitoring, processing, or storage of user data and communications serve a legitimate purpose, such as addressing a specific safety risk or mitigating harm to a specific user or population?[103]

3. Principles of Necessity and Proportionality: Did the company consider all other alternatives to achieving the legitimate aim, and is the chosen policy the least privacy-invasive means of achieving that aim? Is the chosen policy proportionate to the importance of the aim or magnitude of the risk?[104]

Other harms to consider

Cyberattacks

The hacking of XR devices and software could result in a number of harms. First, cyber-attackers could get access to body-based data collected by XR sensors in order to obtain further unauthorized access to systems containing sensitive financial and other personal information. Access to users' biometric information is an irreparable security breach because people cannot change their fingerprints like they can reset passwords.[105]

"The potential dangers of enabling harmful clandestine activities in unmoderated VR spaces justifies a bolder approach to safety, especially at this early stage in the technology's deployment."

Second, malicious actors could use biometric and bodily data to impersonate, defame, or harass individuals.[106] In the same way that companies might exploit body-based data for commercial influence, hackers could use inferential data about individuals' physical and mental vulnerabilities to extort, defame, or manipulate them. A recent security incident involving the theft of user data on Roblox provides an early indication of how bad actors are able to capitalize on security vulnerabilities.[107]

Third, malware attacks could lead to direct physical harm. In 2018, researchers at the Cyber Forensics Research and Education Group conducted a series of stress tests on Valve's SteamVR applications using two consumer headsets, the HTC Vive and the Oculus Rift. Finding vulnerabilities in VR systems, they were able to control the movements of immersed users and lead them to predetermined locations without their knowledge—a type of attack they called the "human joystick." They were also able to alter the hardware's boundaries and trick users into hitting real-world physical objects and walls.[108]

Digital divides

The dissemination of XR technologies to consumers could exacerbate digital divides and inequality due to the high cost of hardware, uneven access to broadband, and early failures to apply accessibility standards across immersive tools and experiences. The cost of VR headsets today ranges from hundreds to thousands of dollars, excluding accessories and the cost of services. Regional disparities in access to high-speed broadband also threaten to perpetuate unequal access to immersive environments, which require a high-speed Internet connection to operate effectively.[109]

On the other hand, immersive technologies have the potential to help reduce accessibility gaps. For example, VR can enable those with mobility limitations to experience new places, provide tailored job training for those with visual or hearing impairments, and help trauma patients regain confidence through exposure therapy.[110] However, the focus of consumer-facing XR platforms to date has not been on improving accessibility outcomes. According to Reginé Gilbert, an engineering professor at NYU who specializes in inclusive design and immersive experiences, companies have generally failed to include people with disabilities or special needs in their design teams. This has resulted in the vast majority of XR features and experiences failing to conform to accessibility standards.[111]

Potential health impacts

The impacts of long-term immersion on physical and mental health are unknown. Some psychologists suspect that prolonged use of VR could trigger symptoms associated with depersonalization or derealization disorder, warning that "heavy users of VR may begin to experience the real world and their real bodies as unreal, effectively shifting their sense of reality exclusively to the virtual environment."[112] Others worry that the ability to choose idealized avatars in VR could alienate people from their actual physical bodies, increasing the sense of detachment and dissatisfaction with reality.[113] These are largely untested hypotheses, and longitudinal studies will be needed to understand the technology's impact on people's, and especially children's, health and wellbeing.[114]

> **"Given the real-time, ephemeral nature of interactions in VR, proactive detection is the only way to catch and address certain dangerous activities like child sexual exploitation and terrorist recruitment before they cause irreparable harm."**

4. Conclusion and Recommendations

The human rights risks posed by XR technologies are not unfamiliar. Ubiquitous data tracking for behavioral advertising is largely an accepted byproduct of engaging in online activity. Cyberbullying and aggression, unfortunately, have become common in many text-based digital forums. Cybersecurity, accessibility, and mental health are subjects of concern in the 2D Internet. Although XR technologies may not introduce entirely new societal risks, they considerably raise the stakes of existing challenges.

Meanwhile, our inadequate regulatory frameworks and technical safeguards leave us ill prepared to manage the risks associated with XR. We should learn from the mistakes of the past. Instead of waiting until this emerging technology reaches mass-market adoption, businesses and policymakers should take action now to mitigate foreseeable harms. Heeding the following recommendations would provide a strong foundation for both sets of stakeholders to address the challenges of XR in the coming years.

Recommendations to XR platforms

1 Commit to a moratorium on the use of body-based data for psychographic profiling

Hardware and software platforms should make a commitment to erase all body-tracking data—including inferential or "abstracted" data derived from eye, face, and limb movements—once it is no longer needed for device functionality. The risks of storing such data greatly outweigh any commercial or other justifications for its use.[115] Erasing body-based data will help prevent the creation of predictive behavioral models, which require aggregation and analysis of data over time.

In addition to restricting their own data storage and use, platforms should ensure that any third parties with access to user data, such as app developers, are subject to the same strict rules. Platforms should make such terms clear in their developer agreements. Further, they should take responsibility for how third parties handle user data by conducting rigorous vetting and periodic audits of all third parties with access to platform APIs.

Finally, platforms should commit to a moratorium on psychographic profiling. Such a use of the technology is unjustifiable and should not be imposed on users as a condition of accessing XR experiences. Any companies that monetize user data should reexamine their business model and explore alternatives that do not harm users' data privacy interests.

2 Provide settings with various options for users to limit their exposure to data collection and safety risks

Platforms should provide clear information about the data collected by each XR application and provide various options for users to limit the type of data collected and processed by their devices, even if exercising those options comes at some cost to their user experience.[116]

Similarly, platforms should provide a variety of settings for users to curate their experience in multi-user environments. Given that effective real-time moderation remains an elusive goal, platforms should develop a greater range of intuitive self-help tools that allow users to manage their exposure to safety risks and take timely action as needed. These include easy-to-use muting, blocking, and reporting functions; customizable personal safety boundaries; intuitive ways to pause or exit an experience; and an option to summon platform moderators to manage problematic interactions in real time.

3 Incorporate privacy, safety, and security best practices into product design and development

Platforms should not wait for risks to manifest in their products before incorporating known best practices. Although the issues around data privacy, safety, and cybersecurity in XR may be daunting, experts in each of these areas have developed engineering tools and design techniques which, if incorporated early in the product-development process, can set platforms up for success.

Privacy-by-design practices include automatic blurring of bystanders' faces and bodies, encryption of user data in transit, and obfuscation of sensitive data using techniques like differential privacy.[117] Safety-by-design principles include adopting third-party rating mechanisms to assess the age-appropriateness of different experiences,[118] integrating positive reinforcement into multi-user environments, and establishing clear escalation pathways and efficient resolution mechanisms for safety issues surfaced by users.[119] Security by design involves setting up cybersecurity defenses against likely attacks, establishing fine-grained authentication and robust control policies for data access, and implementing continuous testing, threat hunting, and vulnerability scans to ensure the resiliency of security systems.[120]

4 Invest in the development of 3D classifiers for automated proactive moderation

Proactive detection using automated systems is the only way to do timely moderation in XR environments where millions of interactions and experiences transpire in real time. To deploy automated moderation effectively and responsibly, XR companies need to develop classifiers for 3D content and continuously test those systems for accuracy and lack of bias.

Reactive moderation in response to user reports of violations is an important part of the content moderation toolkit, but studies on gaming platforms have found that reporting rates are low even when victims suffer acute harassment.[121] XR companies should learn from the experience of game companies, which have begun adopting live voice chat moderation systems to complement human review of user reports.[122] The most prudent approach to moderation in XR similarly involves a combination of automated, real-time moderation and more efficient and standardized user reporting mechanisms, with enough trust and safety specialists to oversee both.

5 Provide clear and accurate information to the public about how XR devices and systems work

To reach widespread consumer adoption, the XR industry needs to earn the public's trust. Given the many betrayals of trust by major social media companies in recent years, XR platforms should prioritize transparency. They should provide clear, comprehensive, and accessible information to users about critical aspects of the technology that might affect them. These include how the company collects and uses data; whether the company monitors and moderates user communication and behavior; and any safety risks to which consumers may be exposed to in specific XR applications.

Given the amount and complexity of information that users are expected to digest, platforms should make greater efforts to provide such information in an engaging, interactive, and digestible format—providing alternatives to text, such as sounds and visuals, to improve accessibility. Rather than drowning users in legalistic documents, they could leverage the immersive nature of the medium to illustrate platforms' policies, features, and affordances in a realistic and dynamic fashion.[123]

6 Include people with diverse abilities and lived experiences in product development teams

XR platforms should seek to reverse, rather than exacerbate, digital divides and inequities. The most effective way to build inclusivity and accessibility into XR products is to ensure that design and engineering teams include people with diverse abilities and backgrounds.[124] These teams should be well versed in accessibility standards for the existing web and should apply them to immersive media through a variety of accommodations and customization options.[125]

Microsoft's SeeingVR product is an example of how XR can have a positive impact on accessibility. SeeingVR comprises a set of tools to make VR applications more accessible to people with limited vision. These tools, which include a magnifying lens, brightness enhancement, and edge overlays for enhanced visibility, are open source and can be applied to existing VR applications by users themselves.[126] Other companies should follow Microsoft's lead and devise similar open-source tools to help accommodate diverse populations in XR environments.

7 Pass comprehensive federal privacy legislation that accounts for XR's data capture capabilities

Privacy advocates in the U.S. have long called for comprehensive federal privacy legislation, which is necessary to harmonize requirements and close loopholes in existing state privacy laws. The advent of XR provides an additional, pressing reason to update privacy protections and enshrine them in legislation that protects consumers nationwide.

The American Data Privacy and Protection Act (ADPPA), a bill that was overwhelmingly approved in a bipartisan vote by the House Energy and Commerce Committee in July 2022, provides a good foundation upon which to build. The proposed law would prohibit companies from collecting sensitive data, such as geolocation and health information, and requires companies to give consumers an opportunity to object before transferring their data to a third party or targeting advertising toward them.[127]

However, the bill needs to be improved to account for the harmful potential uses of body-based data collected by immersive technologies as well as the limitations of notice-and-consent.[128] Specifically, the bill should sharply restrict the use of consumers' bodily data for psychographic profiling.[129] It also should strengthen the concept of "affirmative express consent" by stating that companies must not deprive users of access to an entire product or service when they withhold their consent from specific types of data collection or use.[130] That is, the law should require companies to give users an actual choice to withhold consent by configuring their products and services for various potential levels of data tracking and use.

8 Strengthen federal authority and capacity to oversee digital industries, including XR companies

The Federal Trade Commission (FTC) has a mandate to protect consumers from deceptive statements and unfair practices, a mandate which extends to digital industries, including XR companies. In May 2023, the FTC released a Policy Statement on Biometric Information in which the agency reaffirmed its commitment to combat "unfair or deceptive acts related to the collection and use of consumers' biometric information." Such acts include making "[f]alse or misleading statements about the collection and use of biometric information" and conditioning access to essential goods and services on providing such information. The FTC also noted that businesses could be liable for "[f]ailing to assess foreseeable harms to consumers before collecting biometric information" and "[f]ailing to evaluate the practices and capabilities of third parties."[131] This is a welcome and timely statement which puts XR platforms on notice regarding possible enforcement actions by the FTC.

In order to equip the FTC to carry out its mandate more effectively, Congress should enhance the agency's longstanding consumer-protection authority to shield consumers of online products and services, including XR technologies, from unfair or deceptive practices. Lawmakers also need to allocate adequate additional resources for the agency to carry out this responsibility.[132] Alternatively, Congress should consider creating a stand-alone federal body, such as the Digital Platform Commission proposed by Senator Michael Bennet (D-Colo.)[133] or an agency with even broader jurisdiction over the technology industry such as that proposed by Senators Lindsey Graham (R-SC) and Elizabeth Warren (D-Mass),[134] to ensure robust regulation of digital technologies.

9 Invest in research on health consequences and environmental impact of XR

Little is known about the long-term health impacts of immersive technologies. The government should dedicate funds for the National Institutes of Health to undertake longitudinal studies on the psychological and physiological effects of XR products, especially on children. Likewise, the government should undertake research on the technology's environmental impacts and provide incentives for companies to prioritize sustainability in their product design and deployment.

Endnotes

1 Neal Stephenson, *Snow Crash*, Random House, 1992.

2 https://www.businessinsider.com/mark-zuckerberg-metaverse-losses-top-40-billion-suddenly-ok-meta-2023-7

3 Vivek Nair et al., "Truth in Motion: The Unprecedented Risks and Opportunities of Extended Reality Motion Data," Special Issue on Security and Privacy for the Metaverse, IEEE 2023, at 5, 9.

4 https://www.apple.com/newsroom/2023/06/introducing-apple-vision-pro/; https://variety.com/vip/apple-welcomes-the-world-to-its-augmented-future-1235633852/

5 https://www.news18.com/news/tech/nike-enters-metaverse-with-nikeland-virtual-store-on-roblox-4462814.html

6 Matthew Ball defines the metaverse as a "massively-scaled, interoperable network of real-time rendered 3D virtual worlds which can be experienced synchronously and persistently by an unlimited number of users, each with an individual sense of presence, while supporting continuity of data." https://bigthink.com/series/the-big-think-interview/why-the-metaverse-matters/. Other tech investors and futurists have put forth their own visions for a utopian metaverse. See, e.g., https://time.com/6118513/into-the-metaverse-time-newsletter/; https://www.youtube.com/watch?v=T2qt_5c3RkQ.

7 An interoperable network of immersive spaces would require extensive agreement by major industry players on a set of protocols, or standards, governing the use and transfer of data, currency, assets, content and other information. See, Lau Christensen and Alex Robinson, The Potential Global Economic Impact of the Metaverse, Analysis Group white paper, 2022 at 42.

8 Interview with Louis Rosenberg, on file with author.

9 Louis Rosenberg, "The Metaverse: The Ultimate Tool of Persuasion" in *Metaverse Applications for New Business Models and Disruptive Innovation,* Muhammad Anshari, et al. (eds.). IGI Global, 2023. at 3.

10 https://gamerant.com/roblox-meta-quest-vr/#:~:text=A%20report%20claims%20that%20Roblox,Quest%20VR%20headsets%20in%202023

11 https://www.wsj.com/articles/the-metaverse-is-quickly-turning-into-the-meh-taverse-1a8dc3d0; https://www.theverge.com/2022/10/6/23391895/meta-facebook-horizon-worlds-vr-social-network-too-buggy-leaked-memo

12 https://www.cnbc.com/2023/07/26/metas-reality-labs-has-now-lost-more-than-21-billion.html?utm_source=substack&utm_medium=email; https://www.protocol.com/entertainment/meta-layoffs-reality-labs-metaverse?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axioslogin&stream=top

13 https://www.axios.com/pro/media-deals/2023/03/16/metaverse-funding-plummets-as-investors-favor-generative-ai?utm_source=editorial&utm_medium=social&utm_campaign=pro_edit_regwall_07-22&utm_term=regwall&stream=top

14 In May 2023, the South Korean government launched a $48.3 million fund towards metaverse development. https://hbr.org/2023/05/yes-the-metaverse-is-still-happening?ab=hero-subleft-3. Dubai launched a Metaverse Strategy to attract top metaverse startups, with the aim of making the city one of the world's top ten metaverse economies. https://www.coindesk.com/policy/2022/07/19/dubai-unveils-metaverse-strategy-aims-to-attract-over-1000-firms/. South Africa sponsors its own metaverse, called "Africarare," which offers immersive VR experiences and a marketplace for digital real estate. https://www.globenewswire.com/en/news-release/2022/08/18/2501135/0/en/African-Metaverse-Opens-Up-to-the-World.html. France has even begun exploring public-sector metaverse alternatives through its metaverse consultations, led by the French Directorate General for Enterprise. https://www.tradingview.com/news/cointelegraph:87afc76f0094b:0-france-s-metaverse-consultation-seeks-input-on-alternative-to-tech-giants/.

15 The broad range of projections is likely due to ongoing uncertainty regarding what the metaverse means and whether it will absorb much of the world's economic activity, as some predict. See, e.g., https://www.grandviewresearch.com/press-release/global-metaverse-market; https://www.pwc.com/th/en/press-room/press-release/2020/press-release-29-01-20-en.html; https://www.constellationr.com/research/monetizing-metaverse-economy#:~:text=Furthermore%2C%20Constellation%20predicts%20that%20advances,%2421.7%20trillion%20market%20by%202030.&text=Premium%20content; https://www.mckinsey.com/~/media/mckinsey/business%20functions/marketing%20and%20sales/our%20insights/value%20creation%20in%20the%20metaverse/Value-creation-in-the-metaverse.pdf; https://www.barrons.com/articles/metaverse-web3-internet-virtual-reality-gaming-nvidia-51648744930.

16 Albert Meige et al., "The Metaverse Beyond Fantasy," Blue Shift, Sept. 2022 at 61-63.

17 For instance, the blockchain-based metaverse platform, Decentraland, makes money by issuing MANA tokens, which have a limited supply, and selling virtual real estate. Albert Meige et al., supra, at 65.

18 Existing Law and Extended Reality A Research Symposium at Stanford Law School, January 2023. Recording available at: https://sites.google.com/stanford.edu/xr-2023

19 "XR for Social Impact: A Landscape Review," Games For Change 2020 at 33. See also, "Thinking Ahead About XR," Bipartisan Policy Center, April 2022.

20 Ibid.

21 https://docubase.mit.edu/project/carne-y-arena/

22 "XR for Social Impact: A Landscape Review," supra, at 22-26. See also, https://www.youtube.com/watch?v=FQ_whw6oSv4

23 Ibid at 14, 20; https://www.cnet.com/tech/computing/features/vr-is-revolutionizing-therapy-why-arent-more-people-using-it/

24 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7287864/

25 https://www.bbc.com/news/newsbeat-64862006

26 https://www.lawfaremedia.org/article/artificial-intelligence-virtual-courts-and-real-harms

27 Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight For A Human Future At The New Frontier Of Power*, Public Affairs, 2019.

28 Privacy is enshrined as a human right in the Universal Declaration of Human Rights, article 12.

29 Fiachra O'Brolcháin et al., "The Convergence of Virtual Reality and Social Networks: Threats to Privacy and Autonomy," Springer, 2016.

30 Interview with Dylan Gilbert, on file with author.

31 Mark McGill, "Extended Reality (XR) and the Erosion of Anonymity and Privacy," The IEEE Global Initiative On Ethics Of Extended Reality (XR) Report, 2021.

32 Daniel Berrick and Jameson Spivack, "Understanding Extended Reality Technology & Data Flows," Future of Privacy Forum, Novemeber 2022.

33 While Internet services already have access to private information about individuals—including their education, religion, medical history, political opinions, and family or relationship status—all of this information is provided voluntarily. What distinguishes body-based tracking is the involuntary nature of people's reactions to stimuli and granularity of the data, allowing companies to ascertain not just someone's stated relationship status but details about their sexual inclinations, which the individuals may not wish to reveal.

34 Vivek Nair et al., supra, at 2.

35 Ibid at 4-5.

36 Brittan Heller, "Watching androids dream of electric sheep: immersive technology, biometric psychography, and the law." Vand. J. Ent. & Tech. L. 23, 1, 2020 at 23-24, 28-29, 33. On the capture and potential to exploit brain-sensing data, see https://www.ted.com/talks/nita_farahany_your_right_to_mental_privacy_in_the_age_of_brain_sensing_tech/c. See also https://fpf.org/blog/brain-computer-interfaces-privacy-and-ethical-considerations-for-the-connected-mind/

37 Brittan Heller, "Reimagining Reality: Human Rights and Immersive Technology," Carr Center for Human Rights Policy, Harvard Kennedy School, 2020.

38 RightsCon Summit, Costa Rica 2023. Recording available at: https://rightscon.summit.tc/t/rightscon-costa-rica-2023/events/generative-ai-electric-vehicles-eye-trackers-privacy-and-protection-in-emerging-tech-5kafnGZJC9nynt31dqusaG.

39 Louis Rosenberg, "Ultimate Tool," supra, at 9. See also, James G. Brown et al., "Misinformation in Virtual Reality," *Journal of Online Trust and Safety*, March 2023 at 18.

40 Michael Madary and Thomas K. Metzinger, "Real virtuality: A Code of ethical Conduct. Recommendations for Good Scientific Practice and the Consumers of VR-Technology," Frontiers in Robotics and AI, February 2016 at 5.

41 For example, the EU's Digital Services Act, article 26(1) provides some transparency requirements for online platforms to indicate in a "clear, concise and unambiguous manner and in real time" whether content is advertisement. This regulation arguably applies to 3D online platforms. See https://www.stiftung-nv.de/en/publication/opinion-piece-dsa-also-works-metaverse-if-it-enforced-well

42 Louis Rosenberg, "The Metaverse and Conversational AI as a Threat Vector for Targeted Influence," 2023 IEEE Annual Computing and Communication Workshop and Conference.

43 "Thinking Ahead About XR," supra, at 14; Mark McGill, "Extended Reality (XR) and the Erosion of Anonymity and Privacy," supra, at 6.

44 Interview with Joseph Jerome, on file with author. See also Katitza Rodriguez and Kurt Opsahl, "Augmented Reality Must Have Augmented Privacy," Electronic Frontier Foundation, October 16 2020.

45 https://techpolicy.press/state-bills-arent-enough-the-case-for-national-legislation-on-data-privacy-and-civil-rights/. See also https://www.makingspacepledge.org/u-s-states-are-taking-consumer-privacy-matters-into-their-own-hands/

46 Personal identifying information (PII) typically includes driver's license number, social security number, date of birth, personal financial account number, home address, and other personal information that is used for individual identification. See https://www.dol.gov/general/ppii

47 See, e.g., Wash. Rev. Code Ann. § 19.375.010.

48 Brittan Heller, "Watching androids dream of electric sheep," supra, at 36. Some body-tracking data collected by XR systems, such as eye-gaze tracking, arguably fall under the definition of biometric data. See https://techxplore.com/news/2019-07-deepeyedentification-people-based-micro-eye.html. But this is not the case for other body-based data, such as breath composition. Interview with Brittan Heller, on file with author. For an overview of uses and harms related to consumer profiling or "characterization" based on physical data, see https://fpf.org/blog/fpf-releases-understanding-facial-detection-characterization-and-recognition-technologies-and-privacy-principles-for-facial-recognition-technology-in-commercial-applications/

49 Cal. Civ. Code § 1798.140(o)(1)(K). See also, Cal. Op. Att'y. Gen. No. 20-303.

50 https://oag.ca.gov/privacy/ccpa#sectionb

51 Cal. Civ. Code § 1798.100.

52 Cal. Civ. Code § 1798.140(c).

53 https://gdpr.eu/eu-gdpr-personal-data/

54 GDPR article 9.

55 Interview with Jameson Spivack, on file with author.

56 Helen Nissenbaum, "A Contextual Approach to Privacy Online," Daedalus 2011.

57 Debbie Reynolds interview, on file with author.

58 GDPR article 7.

59 Mark McGill, "Extended Reality (XR) and the Erosion of Anonymity and Privacy," supra, at 17.

60 Ibid at 15.

61 See, e.g., Jordan Belamire's blog post on her experience in QuiVr, https://medium.com/athena-talks/my-first-virtual-reality-sexual-assault-2330410b62ee

62 Mel Slater et al., "The Ethics of Realism in Virtual and Augmented Reality," Frontiers in Virtual Reality, March 3 2020, at 4-5.

63 Ibid. See also, Madary and Metzinger, supra.

64 Mel Slater et al., "Inducing illusory ownership of a virtual body," Frontiers in Neuroscience, Sept. 15, 2009.

65 Lombard and Ditton identified several factors that lead to an increased sense of presence in mediated environments: social richness, realism, the sense of transportation, and perceptual and psychological immersion. See Matthew Lombard and Theresa Ditton, "At the heart of it all: The concept of presence. Journal of computer-mediated communication," 3, 2: JCMC321, 1997.

66 For a more severe hypothetical, see Mark A. Lemley & Eugene Volokh, "Law, Virtual Reality, and Augmented Reality," 166 U. PA. L. REV. 1051, 1063 (2018).

67 https://www.adl.org/resources/report/online-hate-and-harassment-american-experience-2023?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axioslogin&stream=top. See also https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/

68 In a 2018 survey by Extended Mind, 36% of males and 49% of females who regularly used immersive technologies reported experiencing sexual harassment in VR, including being groped, stalked, or receiving a sexually explicit comment. See "Virtual Harassment: The Social Experience of 600+ Regular Virtual Reality (VR) Users, "Extended Mind, April 4, 2018. See also https://www.adl.org/resources/reports/hate-in-social-virtual-reality. For first-person accounts, see https://www.mic.com/articles/144470/sexual-harassment-in-virtual-reality, https://www.businessinsider.com/meta-woman-claims-virtually-groped-metaverse-horizon-venues-2022-1

69 Interview with Toby Shulruff, on file with author. See also Yogesh K. Dwivedi et al., "Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy," International Journal of Information Management 66 (2022), Contribution 7 by Christy M. K. Cheung at 15.

70 https://www.nytimes.com/2021/12/30/technology/metaverse-harassment-assaults.html

71 Michelle Cortese and Jessica Outlaw, "Social And Multi-User Spaces In VR: Trolling, Harassment, And Online Safety," The IEEE Global Initiative On Ethics Of Extended Reality (XR) Report, 2021.

72 https://medium.com/@ellecortese/virtual-healing-bf2b5f0cbf51

73 Interview with Michelle Cortese, on file with author. Michelle Cortese and Andrea Zeller, "Designing Safe Spaces for Virtual Reality: Methods for merging body sovereignty theory into VR design practice" in *Ethics in Design and Communication: New Critical Perspectives,* Bloomsbury Visual Arts: London, 2020.

74 https://nickclegg.medium.com/making-the-metaverse-what-it-is-how-it-will-be-built-and-why-it-matters-3710f7570b04

75 https://www.meta.com/help/quest/articles/horizon/safety-and-privacy-in-horizon-worlds/safe-zone-in-horizon/

76 https://www.meta.com/help/quest/articles/horizon/safety-and-privacy-in-horizon-worlds/use-voice-mode-horizon-worlds/; https://www.meta.com/help/quest/articles/horizon/explore-horizon-worlds/world-chat-horizon-worlds/

77 https://www.meta.com/nl/en/legal/quest/monitoring-recording-safety-horizon/

78 https://www.meta.com/nl/en/legal/quest/monitoring-recording-safety-horizon/; https://www.meta.com/help/quest/articles/horizon/safety-and-privacy-in-horizon-worlds/report-someone-horizon-worlds/

79 https://developer.oculus.com/blog/user-reporting-requirements-developer-tools-updates/

80 https://www.meta.com/help/quest/articles/accounts/privacy-information-and-settings/code-of-conduct-for-virtual-experiences/

81 Facebook Community Standards, https://transparency.fb.com/policies/community-standards/. See also Rafi Lazerson, "A Secure and Equitable Metaverse: Designing Effective Community Guidelines for Social VR," UC Berkeley Center for Long-Term Cybersecurity, CLTC white paper series, Novemeber 2022 at 2.

82 See generally, https://www.adl.org/resources/reports/hate-in-social-virtual-reality

83 Interviews with Andrea Zeller and Michelle Cortese, on file with author.

84 For instance, Riot Games' *League of Legends* has implemented a system in which players are rewarded for sportsmanship with honor points and in-game goods. https://www.scientificamerican.com/article/can-a-video-game-company-tame-toxic-behavior/

85 Interview with Kimberly Voll, on file with author.

86 See, e.g., Meta's approach, https://www.meta.com/help/quest/articles/horizon/safety-and-privacy-in-horizon-worlds/community-guides-in-horizon/

87 Ibid. See also, Brittan Heller, "Watching androids dream of electric sheep," supra, at 47-48.

88 Michelle Cortese and Jessica Outlaw, supra, at 13-14. See also, Lindsay Blackwell et al., "Harassment in Social Virtual Reality: Challenges for Platform Governance," Proc. ACM Hum.-Comput. Interact., Vol. 3, No. CSCW, Article 100, November 2019 at 20.

89 Interview with Michelle Cortese, on file with author.

90 Interview with Brittan Heller, on file with author.

91 "Horizon Worlds Exposed," Center for Countering Digital Hate (CCDH), March 8 2023, https://counterhate.com/wp-content/uploads/2023/03/Horizon-Worlds-Exposed_CCDH_0323.pdf

92 Video clips recorded by the Center for Countering Digital Hate: https://drive.google.com/file/d/1ljyPAwl8lDEurUZBS32fD9BCoNzp9w5P/view; https://drive.google.com/file/d/198YNZAFIDX-GfP4Jlx7LV9-QohaZ-jPE/view; https://drive.google.com/file/d/1tdy9_vvEQk2bhr6A7JNWP28rQHX-W4gQ7/view

93 https://drive.google.com/file/d/1PTceJA5TNvNdjYkZKW4T3XZYdP2ArX-hy/view

94 "Horizon Worlds Exposed," supra, at 2.

95 https://www.nytimes.com/2023/06/16/technology/meta-virtual-reality-headset-children-safety.html?utm_source=substack&utm_medium=e-mail

96 https://www.ft.com/content/d72145b7-5e44-446a-819c-51d67c-5471cf?utm_source=dlvr.it&utm_medium=twitter

97 https://communityforums.atmeta.com/t5/Talk-VR/Y-son-was-violently-threatened-and-continuously-harassed-on/m-p/1029083

98 Interview with Joseph Jerome, on file with author.

99 There are different types of age assurance methods with varying levels of certainty – age verification being only one of them – and each comes with tradeoffs. See Scott Brennen and Matt Perault, "Keeping Kids Safe Online: How Should Policymakers Approach Age Verification?" June 2023 Policy Paper.

100 Interview with Patrick Lin, on file with author. The author would also like to thank Kerin McCauley for reinforcing this point. Furthermore, the collection of data for age assurance could be made minimally privacy invasive by processing and storing the age assurance data on users' devices rather than on companies' servers. Interview with Jameson Spivack, on file with author.

101 As Scott Babwah Brennen and Matt Perault from the Center on Technology Policy at the University of North Carolina Chapel Hill observe in a policy paper on age assurance, "there are no silver bullets to the problem of age verification." But businesses and policymakers can still approach the problem responsibly by engaging in well-informed cost-benefit analysis and choosing policies that strike a reasonable balance among the competing interests of privacy, safety, and equity. See Scott Brennen and Matt Perault, "Keeping Kids Safe Online," supra, at 2.

102 This three-part test is contained in Article 19 of the International Covenant on Civil and Political Rights (ICCPR) and relates to permissible limitations on freedom of expression. The same three-part test can be applied to the right to data privacy. See, e.g., UN Human Rights Council Resolution on the right to privacy in the digital age, A/HRC/RES/42/15.

103 See UN General Assembly, Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms, A/77/196, July 20 2022, para. 59.

104 Ibid at para. 83.

105 "Thinking Ahead About XR,"supra, at 13.

106 Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act, May 2023.

107 In 2022, a hacker stole internal Roblox documents and player data, which they threatened to leak unless given digital currency. https://www.cshub.com/attacks/articles/data-breaches-on-gaming-sites-are-becoming-more-common. In an earlier security incident in 2018, another hacker infected the Roblox system with ransomware and programmed characters to gang-rape a seven-year-old girl. https://techcrunch.com/2018/07/18/roblox-responds-to-the-hack-that-allowed-a-childs-avatar-to-be-raped-in-its-game/

108 Peter Casey et al., "Immersive Virtual Reality Attacks and the Human Joystick," IEEE Transactions on Dependable and Secure Computing, Vol. 18, No. 2, March/April 2021.

109 "Thinking Ahead About XR," supra.

110 Ibid.

111 Interview with Reginé Gilbert, on file with author. Gilbert, along with a group of students, examined over 60 tools and features in XR applications and found that "only a tiny portion were made with accessibility in mind."

112 Madary and Metzinger, supra, at 14.

113 Dwivedi et al., supra. Contribution 6 by Giampaolo Viglia at 14-15.

114 Madary and Metzinger, supra, at 8.

115 Katitza Rodriguez and Kurt Opsahl, supra.

116 https://uxdesign.cc/meta-quest-pro-falls-short-on-biometric-protections-ba48db35637f

117 Vivek Nair et al., "Truth in Motion," supra, at 6-7.

118 For instance, Meta uses the International Age Rating Coalition (IARC), a global age classification process for digital games and mobile apps, to rate Quest apps. https://www.oculus.com/safety-center/

119 https://www.esafety.gov.au/industry/safety-by-design/principles-and-background

120 Other recommended cybersecurity practices for XR companies include: designing devices so they have enough capacity to store sensitive data locally (on the device itself rather than in a centralized repository); configuring sensors so they automatically obfuscate sensitive user data and personal information before it is transferred to external servers; encrypting any data that must be stored in a centralized location; deleting user data once it is no longer needed for device functionality; implementing strong endpoint security through VPNs, proxies, and antimalware software; restricting third-party access to user data, including by improving the security of developer APIs and regularly auditing third-party practices around data handling; devising advanced anomalies detection abilities; and reinforcing fine-grained identity and authentication standards. See https://www.uscybersecurity.net/csmag/a-wrinkle-in-metaverse/

121 https://bhr.stern.nyu.edu/tech-gaming-report

122 https://www.modulate.ai

123 Interview with Joseph Jerome, on file with author.

124 Interview with Reginé Gilbert, on file with author.

125 See the World Wide Web Consortium's Web Content Accessibility Guidelines, https://www.w3.org/TR/WCAG21/

126 Reginé Gilbert, *Inclusive Design for a Digital World - Designing with Accessibility in Mind,* Apress, 2019 at 207. For the open-source code, see https://github.com/microsoft/SeeingVRtoolkit

127 ADPPA Sect 204(c), available at: https://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS-1178152rh.pdf. See also, https://techpolicy.press/state-bills-arent-enough-the-case-for-national-legislation-on-data-privacy-and-civil-rights/

128 https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/

129 Brittan Heller, "Reimagining Reality: Human Rights and Immersive Technology," supra, at 19.

130 See ADPPA Sec 2(1) "Affirmative express consent."

131 FTC Policy Statement, supra.

132 https://techpolicy.press/state-bills-arent-enough-the-case-for-national-legislation-on-data-privacy-and-civil-rights/

133 https://www.bennet.senate.gov/public/index.cfm/2022/5/bennet-introduces-landmark-legislation-to-establish-federal-commission-to-oversee-digital-platforms; https://www.lawfareblog.com/digital-regulator-must-be-empowered-address-ai-issues

134 Digital Consumer Protection Commission Act draft text, https://www.warren.senate.gov/imo/media/doc/DCPC%20Section-By-Section.pdf

NYU Stern Center for Business and Human Rights
Leonard N. Stern School of Business
44 West 4th Street, Suite 800
New York, NY 10012
+1 212-998-0261
bhr@stern.nyu.edu
bhr.stern.nyu.edu

Center for Business
and Human Rights