MINDEROO
CENTRE FOR
TECHNOLOGY
& DEMOCRACY

SECURING THE METAVERSE:

ADDRESSING HARMS IN EXTENDED REALITY

Shannon Pierson
July 2023

July 2023

Minderoo Centre for Technology and Democracy

The Minderoo Centre for Technology and Democracy is an independent team of academic researchers at the University of Cambridge, who are radically rethinking the power relationships between digital technologies, society and our planet.

www.mctd.ac.uk

DOI: **doi.org/10.17863/CAM.99564**

CONTENTS

FOREWORD

How do we secure the metaverse?

This report from Shannon Pierson, an affiliate at the Minderoo Centre for Technology and Democracy at the University of Cambridge, explores ways to tackle harms presented by the advancement of extended reality (XR) technologies.

Thanks to Shannon's extensive research into online harms at scale on social media platforms, this report maps how to address the harms presented by XR.

From the governance of interconnected, persistent computer-generated worlds, to the biometric data privacy concerns they present, and cybersecurity obstacles in XR technology today, this report signals what problems lie ahead for a fully realised metaverse.

At the Minderoo Centre for Technology and Democracy, at the University of Cambridge, we study how digital technology is transforming society to ensure democratic accountability over the increasing power of tech across the globe.

Our research is anchored in creating ways to build capacity in how we as a society can hold tech power systems to account, to create a just future.

We hope that this report will be useful to a wide range of different stakeholders in scrutinising metaverse developments, and address how we can use regulatory and legislative power today, to protect against the entrenchment of harmful metaverse developments that could impact us and future generations.

Prof. Gina Neff

Executive Director,
Minderoo Centre for Technology
and Democracy

EXECUTIVE SUMMARY

Advancements in extended reality (XR) technologies are bridging the gap between the physical and virtual world and propelling the concept of a "metaverse"—a network of interconnected, persistent computer-generated worlds—closer to fruition.

Applications of XR systems are poised to disrupt and transform the global digital economy, with some forecasting the metaverse to grow into a £3.975 trillion industry by 2030.[1] Beyond gaming, XR and metaverse technologies have the potential to revolutionise various industries: including education and skills training, healthcare, entertainment, and the future of work and personal productivity.

The breadth and intimacy of the personal information collected by XR devices is unlike anything yet seen in another consumer-grade product. Emerging Social VR platforms remain largely unmoderated virtual spaces rampant with toxicity and online abuse.

Currently, few guardrails are in place to ensure that the development of XR technologies progresses responsibly and prioritises user safety and privacy. Policymakers must begin considering regulation that addresses the risks of these products and services before they enter the mainstream.

If left unaddressed, these problems will become entrenched into metaverse infrastructure and business models in ways that will be difficult, if not impossible, to untangle.

This report provides an assessment of possible harms and suggests policy recommendations to mitigate them. We examine the governance, biometric data privacy, and cybersecurity obstacles in XR technology today in order to signal what problems lie ahead for a fully realised metaverse.

From our findings we propose interventions to improve user safety and privacy within metaverse platforms and technologies. For the UK, we suggest ways to use the Online Safety Bill and existing privacy, security and consumer protection laws to address harms in metaverse mediums.

1. McKinsey & Company, *Value Creation in the Metaverse: the Real Business of the Virtual World* (June 2022) <https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/value-creation-in-the-metaverse> [accessed 5 June 2023], p. 6. Figure converted to GBP from $5 trillion, June 2023.

Our report is structured as follows:

Section I: Metaverse Platform Governance

Findings:

- Platforms' moderation tools do not sufficiently protect users — particularly children and marginalised groups — from harms that are pervasive in Social VR. As a result, Social VR spaces do not uniformly enforce their rules.
- Social VR platforms fail to enforce age restrictions and ensure age-appropriate spaces for children separated from adults. Children frequently encounter and experience bullying, sexist and racist hate speech, simulated sexual interactions, and sexual harassment.
- Generative AI will scale content creation in the metaverse and make it easier for bad actors to create immersive experiences that harm, mislead and manipulate.

Recommendations to improve metaverse platform governance:

- Policymakers must establish expectations that companies actively monitor Social VR environments.
- Expand the definition in the UK's Online Safety Bill for what qualifies as 'content' with respect to XR.
- Regulators, including the UK's Ofcom, should be proactive about metaverse technologies.

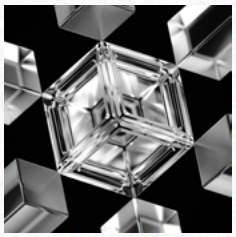
Section II: Biometric Data

Findings:

- Involuntary biometric responses tracked by XR devices can divulge sensitive personal information, including data that can indicate medical conditions, sexual orientation, and identity.

Recommendation to protect people in the metaverse:

- Existing privacy, security and consumer protection laws need to be re-evaluated and updated to ensure that they apply across metaverse devices and experiences.



Section III: Cybersecurity

Findings:

- Cybercriminals have begun exploiting the emerging metaverse's non-fungible token (NFT) market to profit from investment fraud scams, money laundering schemes, and the exchange of illicit materials.
- XR devices share many of the same cybersecurity vulnerabilities that other consumer-grade devices, including IoT devices, have and may require better authentication mechanisms and stronger encryption.

Recommendations to address cybersecurity risks:

- Governments and industry must commit to embedding security and privacy by design into metaverse products and services.

INTRODUCTION

Applications of extended reality (XR) systems open up a world of exciting possibilities in the Web 3.0 digital economy.

XR technology has the potential to revolutionise various industries: including education and skills training, healthcare, entertainment and gaming. XR systems provide opportunities to reshape the future of work and enhance personal productivity.

Today, few guardrails exist to ensure that the development of XR technologies progresses responsibly and prioritises user safety and privacy. The breadth and intimacy of the personal information collected by XR devices is unlike anything yet seen in consumer products.

Emerging Social Virtual Reality (VR) platforms remain largely unmoderated, resulting in toxic virtual spaces rampant with online abuse.

Policymakers must begin considering regulation that addresses the risks of these products and services before they enter the mainstream.

If these problems become entrenched into metaverse infrastructure and business models it will be difficult, if not impossible, to untangle and deal with them.

This report cuts through the hype and dismissals surrounding XR technologies and Social VR platforms to provide an assessment of the harms manifesting today and recommendations to mitigate them.

We present a status report on the governance, data privacy, and cyber-security challenges in XR technology today to signal what problems lie ahead for a fully realised metaverse. We propose possible interventions for policymakers and technology companies to design safer systems.

What is the Metaverse?

The term 'metaverse' describes a vision for the future of the internet: a network of interconnected, persistent computer-generated worlds facilitated by and accessed through virtual reality (VR) and augmented reality (AR) devices.[2]

In the metaverse, users can enter three-dimensional, immersive virtual spaces and interact with one another in real time to socialise, play, collaborate, and exchange digital goods.[3] The metaverse is live and never switches off, and users can navigate seamlessly between worlds.

Many technological hurdles must be overcome before these visions for the metaverse are fully realised.[4] While the metaverse may be years away, technology companies like Meta, ByteDance, Microsoft, Tencent, Apple, HTC, and others have invested hundreds of billions of pounds into developing XR technology.

They are currently carving out portions of the emerging XR market by buying up XR hardware and software companies and securing XR patents.[5] McKinsey forecasts that the metaverse will grow into a £3.975 trillion industry by 2030.[6]

The metaverse is often described as the next iteration of the internet. Companies like Apple and Meta push forward the notion that mixed reality (MR) headsets could eventually replace smartphones.[7]

Looking beyond the hype, the metaverse continues to be defined and take shape as the technology matures and adoption increases.

Still, it remains to be seen how the metaverse will be constructed and governed. Some visions for the metaverse see it consisting of decentralised ownership similar to Web 3.0 technologies. Today's powerful platform companies could coalesce industry power in the hands of a few corporate entities.

There are three competing models for how metaverse platforms will be arranged and governed in the future: centralised, multiverse, and decentralised. These directions will have implications for what levers companies and policymakers have for governing and regulating metaverse technologies.

2. Georg David Ritterbusch and Malte Rolf Teichmann, 'Defining the Metaverse: A Systematic Literature Review', *IEEE Access*, 11 (2023), 12368–12377, doi: 10.1109/ACCESS.2023.3241809.

3. Sam Gilbert, 'The Political Economy of the Metaverse', *IFRI: French Institute of International Relations*, Briefings de l'Ifri, 20 June 2022 <https://www.ifri.org/en/publications/briefings-de-lifri/political-economy-metaverse> [accessed 16 June 2023].

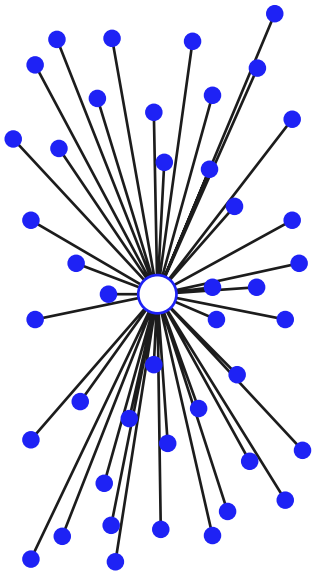
4. Gilbert, 'The Political Economy of the Metaverse'.

5. Federal Trade Commission, 'FTC Seeks to Block Virtual Reality Giant Meta's Acquisition of Popular App Creator Within', Federal Trade Commission, 27 July 2022 <https://www.ftc.gov/news-events/news/press-releases/2022/07/ftc-seeks-block-virtual-reality-giant-metas-acquisition-popular-app-creator-within> [accessed 15 April 2023].

6. McKinsey & Company, *Value Creation in the Metaverse*, p. 6.

7. Michael E. Porter and James E. Heppelmann, 'Why Every Organization Needs an Augmented Reality Strategy', *Harvard Business Review*, Nov–Dec 2017, 46–57 <https://hbr.org/2017/11/why-every-organization-needs-an-augmented-reality-strategy> [accessed 6 February 2020]; Alex Heath, 'This is Meta's AR / VR Hardware Roadmap for the Next Four Years', *The Verge*, 1 March 2023 <https://www.theverge.com/2023/2/28/23619730/meta-vr-oculus-ar-glasses-smartwatch-plans> [accessed 10 April 2023]; José Adorno, 'Apple Execs Reportedly Think Mixed Reality Headset Could Replace the iPhone', *BGR*, 17 April 2023 <https://bgr.com/tech/apple-execs-reportedly-think-mixed-reality-headset-could-replace-the-iphone/> [accessed 1 June 2023].

Visions for Metaverse Governance

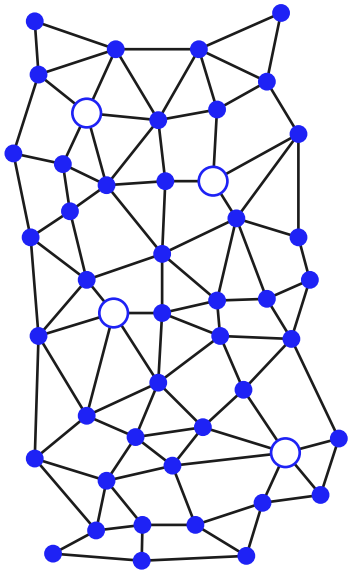


CENTRALISED

One entity exclusively owns, operates, and governs a centralised enclosed network of virtual worlds.

The central entity owns all user-generated content and collects and stores user-interaction data.

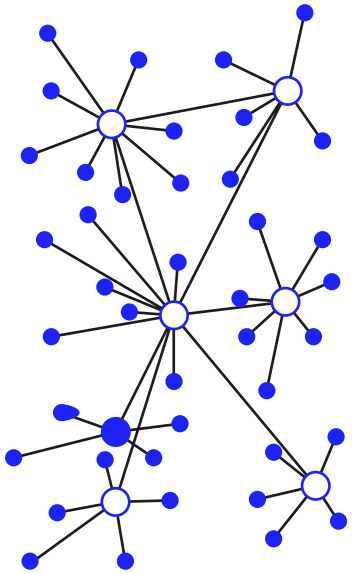
Users cannot control or own pieces of the virtual environment themselves.



MULTIVERSE

Multiple entities own, operate, and govern separate but interconnected networks of virtual worlds.

Each world is enclosed and has its own governing structure, economy, and unique user experience.



DECENTRALISED

Users collectively own, operate, and govern a decentralized interconnected, interoperable network of virtual worlds through blockchain technology.

There is no central authority enforcing rules, but users who own digital property in the form of non-fungible tokens (NFTs) have decision-making power over their respective domains.

What is Extended Reality? Augmented, Mixed, and Virtual Reality

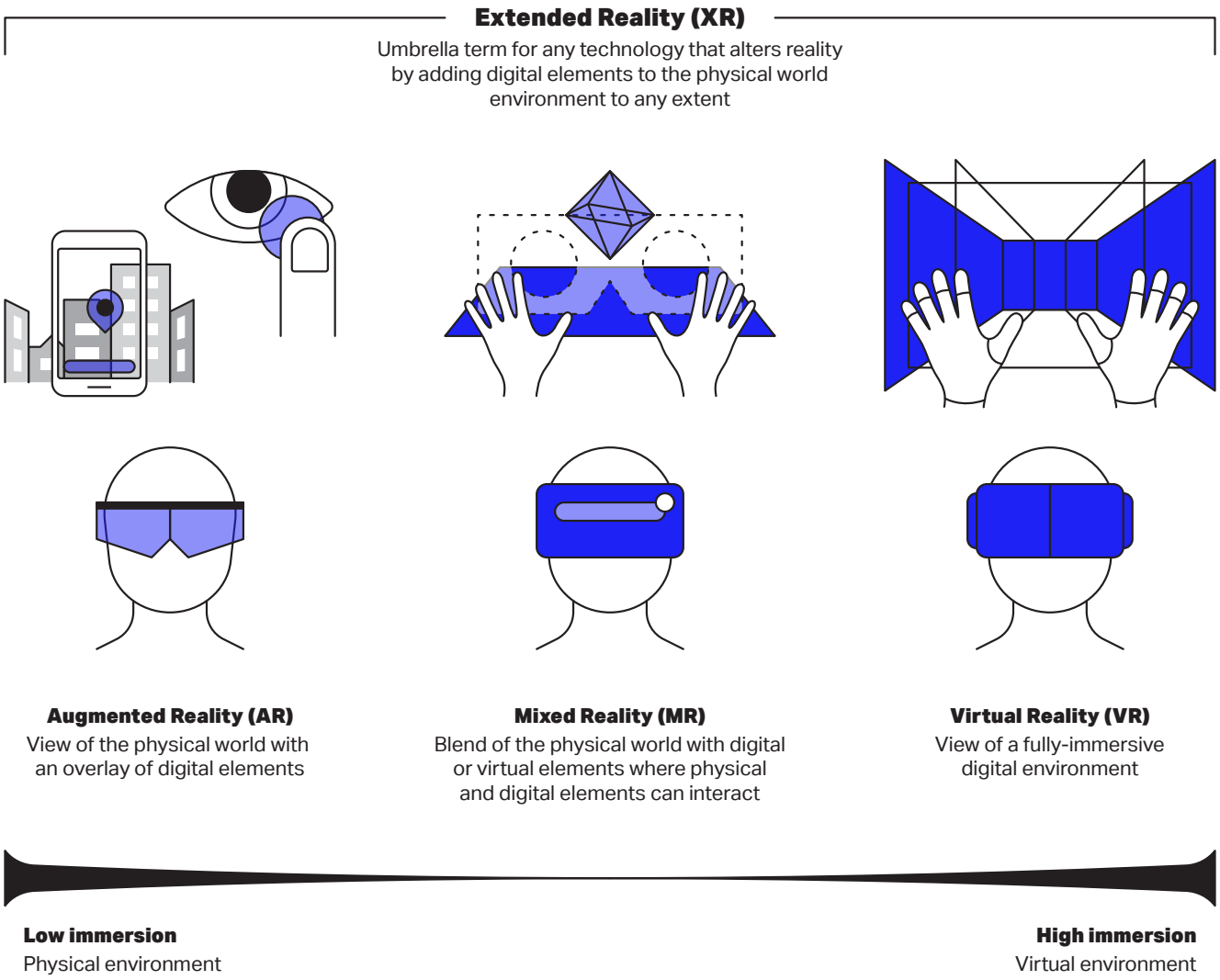


Figure 1: High resolution designer rendition of where XR technologies sit on the virtual reality continuum in terms of immersion. Adapted from research prepared by Laia Tremosa, the Interaction Design Foundation, Paul Milgram, and Fumio Kishino.

8. Tidjane Tall, 'Augmented Reality vs Virtual Reality vs Mixed Reality', *Toptal*, 21 September 2021, <https://www.toptal.com/designers/ui/augmented-reality-vs-virtual-reality-vs-mixed-reality> [accessed March 4 2023]; Laia Tremosa, 'Beyond AR vs. VR: What is the Difference between AR vs. MR vs. VR vs. XR?', *Interaction Design Foundation*, 2022 <https://www.interaction-design.org/literature/article/beyond-ar-vs-vr-what-is-the-difference-between-ar-vs-mr-vs-vr-vs-xr> [accessed 20 January 2023].

SECTION I: METAVERSE PLATFORM GOVERNANCE

Today, there are precursors to a fully functional, persistent, and cross-platform metaverse.[9] These are Social VR platforms, which are XR apps focused on social networking and social gaming experiences.

Social VR platforms like Horizon Worlds, Roblox, VRChat, and Rec Room provide a glimpse of the governance and moderation obstacles that lie ahead for a fully realised metaverse.

Evaluation of the harms and governance challenges manifested in Social VR today can offer perspective on and lessons for regulators thinking ahead to how to regulate the metaverse to come.

Content Moderation Obstacles in Social VR

When considering how the Online Safety Bill applies to metaverse platforms, it is important to understand what distinguishes Social VR from the traditional social media platforms the legislation was written for. Social VR is distinct from social media, and user-generated content and online harassment manifest very differently in these respective mediums.

What constitutes user-generated content in Social VR is far more diverse and complex compared to what we have seen previously on social media.

One reason is that the content in Social VR is three-dimensional, not two-dimensional. Social VR content can include avatar skins, virtual objects, virtual worlds, and user-made games.

Social VR users actively experience a fully immersive content environment where they can interact directly with content and other people by walking around in and exploring virtual worlds. Social VR is all about user activity, which occurs synchronously and involves actions taken by players (i.e., jumping, waving, dancing).

9. 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), 102542, doi: 10.1016/j.ijinfomgt.2022.102542 [version of record 16 July 2022].

User interaction in Social VR is physical, as user avatars can enter each other's personal space and virtually touch each other in ways that can trigger physiological and emotional responses in users.[10]

XR headsets and haptic gear, which are wearable devices that provide tactile feedback to simulate the sensation of touch, engage users' senses in order to give players the illusion of presence in virtual environments, and the perception that an avatar body is their own.[11]

In Social VR, users' physical actions are translated into virtual simulations, enabling them to 'touch' and affect virtual objects and other users. The illusion is further supported by the integration of immersive details like spatial audio, haptic touch, and non-verbal communication cues (i.e., representing a user's facial expressions on their avatar).[12]

Part of what makes VR so convincing is that simulations elicit physiological responses, making experiences like standing before a virtual cliff heart-pounding or climbing through an enclosed virtual space feel claustrophobic.

However, the immersive nature of XR can make perceived threats to one's physical safety feel physically and psychologically real.[13]

This 'physicalised nature' of Social VR has created new immersive forms of online harassment.[14] Harassment in XR manifests in the form of simulated physical behaviours intended to disturb or violate the personal space of other players. Harassment can involve trolling behaviour, where users deliberately irritate a target enough to make them leave a virtual space by circling or stalking them, blocking their view, or screaming in their vicinity.

10. Guo Freeman *et al.*, 'Disturbing the Peace: Experiencing and Mitigating Emerging Harassment in Social Virtual Reality', *Proceedings of the ACM on Human-Computer Interaction*, 6 (2022), 1–30 <https://dl.acm.org/doi/pdf/10.1145/3512932> [accessed 1 June 2023]; Anna Felnhofer *et al.*, 'Is Virtual Reality Emotionally Arousing? Investigating Five Emotion Inducing Virtual Park Scenarios', *International Journal of Human-Computer Studies*, 82 (2012), 48–56, doi: 10.1016/j.ijhcs.2015.05.004.

11. Alice Chirico and Andrea Gaggioli, 'When Virtual Feels Real: Comparing Emotional Responses and Presence in Virtual and Natural Environments', *Cyberpsychology, Behavior, and Social Networking*, 22 (2019), 220–226, doi: 10.1089/cyber.2018.0393.

12. Meta, Natural Facial Expressions Privacy Notice (November 2022) <https://www.meta.com/en-gb/help/quest/articles/accounts/privacy-information-and-settings/natural-facial-expressions-privacy-notice/> [accessed 10 March 2023]; Tijmen Verhulsdonck, Dario Kneubuhler, Inaki Navarro Oiza, Ian Sachs, and Kiran Bhat, 'Real Time Facial Animation for Avatars', *Roblox*, 22 March 2022 <https://blog.roblox.com/2022/03/real-time-facial-animation-avatars/> [accessed 10 March 2023].

13. Kirill A. Fadeev *et al.*, 'Too Real to Be Virtual: Autonomic and EEG Responses to Extreme Stress Scenarios in Virtual Reality', *Behavioural Neurology*, 2020 (2020), 1–11, doi: 10.1155/2020/5758038.

14. Freeman *et al.*, 'Disturbing the Peace'.

More extreme cases of harassment can involve simulated touching and violence, or enactment of self-harm or suicide.[15]

User-to-user verbal communication occurs primarily over voice chat and, therefore, is audio and not text-based. Many gamers prefer using voice chat during live multiplayer games, however it is a notorious vector for toxic and violent speech.[16] Voice chat use in VR creates pathways for online harassment, as users in public virtual spaces often overhear hate speech, verbal attacks, or yelling and screaming occurring in their avatar's vicinity. While users can mute or block aggressors individually, racially-charged insults and hate speech cannot be unheard, and affect users in the nearby area.

Repeated exposure to hate speech communicated via the voice chat feature represents a collective harm as it makes virtual spaces unwelcoming for marginalised groups, and research has shown it may reduce our ability to empathise with others.[17]

15. Freeman *et al.*, 'Disturbing the Peace'.

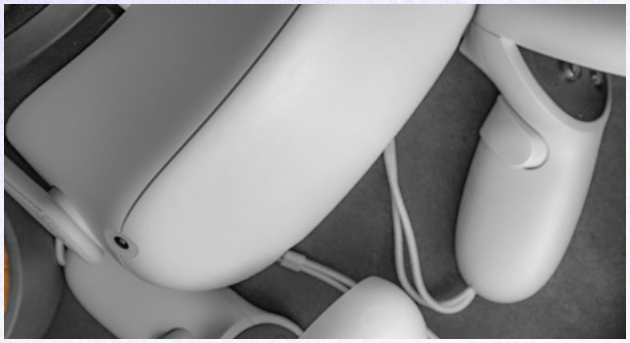
16. Otto Söderlund, 'Voice Chat is Popular with Gamers — It's also the Top Source of Toxic Behavior — New Report', *Speechly*, 8 March 2023 <https://www.speechly.com/blog/voice-chat-is-popular-with-gamers-its-also-the-top-source-of-toxic-behavior-new-report> [accessed 15 May 2023].

17. Agnieszka Pluta *et al.*, 'Exposure to Hate Speech Deteriorates Neurocognitive Mechanisms of the Ability to Understand Others' Pain', *Scientific Reports*, 13 (2023), 1–12, doi: 10.1038/s41598-023-31146-1.

Case Study: Cyberbullying and Hate Speech

Bullying and hate speech are pervasive in Social VR. Racism, homophobia, antisemitism, and other forms of online hate thrive in these largely unmoderated, unmonitored public virtual social spaces.

Conversations occur in real-time over voice chat, uncensored and without leaving a lasting record. The lack of rule enforcement, the anonymity afforded by the platforms, and toxic gaming culture embolden users to spread toxicity uninhibited.[18]



Social VR is consequently a hotbed for online vitriol, where virtual public spaces are made uninhabitable for women, Black, Asian and minority ethnic (BAME), and other marginalised communities.[19] Users are targeted with identity attacks based upon their voice and their avatar's presented gender and ethnicity.

A Channel 4 Dispatch investigation into abuse on Social VR platforms found extreme sexist, racist, and homophobic hate speech to be prevalent on VRChat.[20] Hate speech and openly racist and antisemitic conversations were a commonplace feature of public virtual rooms. An investigator posing as a thirteen-year-old easily accessed adult-only spaces and became the target of racialized harassment and slurs.

The hate speech was so casual and omnipresent that investigators gradually became desensitised to its severity.

18. Rachel Kowert, 'Dark Participation in Games', *Frontiers in Psychology*, 11 (2020), doi: 10.3389/fpsyg.2020.598947.

19. Sylvia Varnham O'Regan and Mathew Olson, 'In Facebook's VR Headset, Racism and Other Abuses Showed Up "Like Clockwork"', *The Information*, 12 November 2021 <https://www.theinformation.com/articles/in-facebooks-vr-headset-racism-and-other-abuses-showed-up-like-clockwork> [accessed 10 March 2023].

20. 'Inside the Metaverse: Are You Safe? | Dispatches | Channel 4 Documentaries', *YouTube*, uploaded by Channel 4 Documentaries, 1 October 2022 <https://www.youtube.com/watch?v=ssgLSky8hfg> [26 February 2023].

Case Study: Virtual Sexual Harassment

Across the internet, women are subject to disproportionate amounts of online abuse, which is often gendered and sexualised in nature.[21] Sexual harassment and abuse against women has already become a widespread problem in Social VR.

Women commonly experience simulated groping and other unwanted sexual interactions and communication. Some Social VR users report experiencing up to three instances of gendered and sexualised harassment a week.[22]

VR brings women's bodies into virtual environments via female-presenting avatars and female users' voices. Women's gender makes them targets for unwanted sexual attention and interactions with other users in Social VR spaces.

This manifests in the form of verbal threats to women's physical safety, including:

- Descriptions of rape and sexual violence
- Unwanted virtual touching
- Non-consensual simulated virtual sexual acts

For example, a beta tester for Horizon Worlds reported that a stranger groped her avatar's body in a public plaza while surrounding avatars egged on the harassment.[23] A BBC investigative reporter posing as a thirteen-year-old girl on VRChat received sexual propositions from adults and encountered real voices yelling aggressive rape threats in her vicinity.[24]

Sexual harassment in VR can cause non-trivial psychological harm to users.[25] Some women who have experienced 'virtual sexual assault' report feeling disoriented and that the abuse was physically happening to them.[26] Gendered and sexualised harrassment in VR is immersive and visceral, given that players' bodies and minds can often react to virtual stimuli in VR as they would to physical stimuli.[27]

This harm may be compounded with the addition of haptic body gear, which enables users to have a more immersive experience in VR. For example, a forty-three-year-old woman experienced her avatar's chest being groped in the first-person shooter game Population One while wearing a haptic vest. The haptic device provided vibration feedback to her body and made the harassment feel physically real.[28]

21. Sarah Sobieraj, *Credible Threat: Attacks against Women Online and the Future of Democracy* (Oxford: Oxford University Press, 2020), doi: 10.1093/oso/9780190089283.001.0001.

22. Angus Crawford and Tony Smith, 'Metaverse App Allows Kids into Virtual Strip Clubs', *BBC News*, 23 February 2022 <https://www.bbc.co.uk/news/technology-60415317> [accessed 12 February 2023].

23. Alex Heath, 'Meta Opens Up Access to its VR Social Platform Horizon Worlds', *The Verge*, 9 December 2021 <https://www.theverge.com/2021/12/9/22825139/meta-horizon-worlds-access-open-metaverse> [accessed 16 February 2023].

24. Crawford and Smith, 'Metaverse App Allows Kids into Virtual Strip Clubs'.

25. John Danaher, 'The Ethics of Virtual Sexual Assault', in *The Oxford Handbook of Digital Ethics*, ed. Carissa Véliz (online edn, Oxford Academic, 10 November 2021), doi: 10.1093/oxfordhb/9780198857815.013.14.

26. Brittan Heller, 'Reimagining Reality: Human Rights and Immersive Technology', *Carr Center for Human Rights Policy, Harvard Kennedy School*, Carr Centre Discussion Paper Series, 2020.008, 12 June 2020 <https://carrcenter.hks.harvard.edu/publications/reimagining-reality-human-rights-and-immersive-technology> [accessed 16 June 2023].

27. Fadeev *et al.*, 'Too Real to Be Virtual'.

28. SumofUs, *Metaverse: Another Cesspool of Toxic Content* (May 2022)

Social VR's immersive, live medium complicates policing Social VR platforms. All conversations and physical interactions between users are synchronous, unfiltered, and ephemeral — meaning interactions happen quickly and are not often represented by a lasting digital record.

This medium makes it more difficult for platforms to monitor and detect abuse, as well as prevent hate speech and harassment in the metaverse environments they host. The policy frameworks and content moderation regimes developed over the years to govern social media platforms and enforce community guidelines at scale have not translated seamlessly to virtual worlds.

The automated methods typically used to moderate content on social media, such as natural language processing (NLP), machine learning models, and image and video recognition software, are text, image, and video-based methods not directly applicable to immersive environments.

For example, hate speech-detection models are text-based. However, the lack of a text-based, searchable digital record of verbal or non-verbal interactions between users makes it challenging for companies to monitor and moderate abuses at scale.

Automated monitoring and moderating of verbal communication in Social VR would require reliable audio-based language classification models, which are still under development.[29] Some social VR platforms have begun integrating voice moderation software capable of:

- Detecting and contextualising toxic speech spoken in real-time
- Escalating it to immediate action
- Identifying the worst offenders[30]

However, not all platforms use this intervention because it is costly and slow, given the great deal of computing power required to perform it and the large data processing costs.[31] Also, live voice chat moderation tools to date have low accuracy.[32]

29. Midia Yousefi and Dimitra Emmanouilidou, 'Audio-Based Toxic Language Classification Using Self-Attentive Convolutional Neural Network', *29th European Signal Processing Conference (EUSIPICO)* (August 2021), doi: 10.23919/EUSIPCO54536.2021.9616001.

30. Dean Takahashi, 'Modulate's ToxMod Uses AI to Scan Game Voice Chat for Toxic Speech', *Venture Beat*, 14 December 2020 <https://venturebeat.com/business/modulates-toxmod-uses-ai-to-scan-game-voice-chat-for-toxic-speech/> [accessed 23 February 2023].

31. Lee Davis, 'Best Practices for Voice Chat Moderation', *Spectrum Labs*, 29 June 2020 <https://www.spectrumlabsai.com/the-blog/best-practices-for-voice-chat-moderation> [accessed 1 May 2023].

32. Otto Söderlund, 'Why Games Need Better Voice Chat Moderation', *Speechly*, 24 October 2022 <https://www.speechly.com/blog/why-games-need-better-voice-chat-moderation> [accessed 15 May 2023].

Social VR platforms police their platforms and enforce rules primarily through human moderation.[33]

VR moderation strategies generally involve stationing human moderators in public virtual spaces and rely on user reporting to flag abusive user interactions and user-generated content. Human moderators then manually review reports on a case-by-case basis for platform codes of conduct violations.[34]

Other VR moderation approaches allow for community moderation, where users adjudicate violations and vote to eject users for violating standards.[35]

Dependence on user reporting creates other obstacles. Reporting abusive behaviour is often a burden for users, placing the onus on targets and parents to detect and report abuse during or after the harm has already been inflicted.

Reporting instances of bullying, hate speech, and sexual harassment often requires written descriptions and screenshots or video recordings of the interaction and abuser(s) user IDs — which users may not have documented mid-attack.[36] While it varies from platform to platform, targets often never receive word back on the outcome of their reports.[37]

These interventions offer spotty moderation coverage at best and are not operable at scale. This means Social VR spaces routinely fail to uniformly enforce their rules across the platform. Moreover, the human moderation approach is reactive rather than proactive and preventative. Generally, this approach is unsustainable for long-term growth.

Copy-pasting interventions deployed for social media to the Social VR platforms does not work perfectly. Therefore, Social VR companies must tailor policy frameworks and pioneer scalable moderation techniques to spatial mediums to govern their platforms — and the future metaverse — effectively.

33. James G. Brown, Jeremy N. Bailenson, and Jeffrey Hancock, 'Misinformation in Virtual Reality', *Journal of Online Trust and Safety*, March 2023 <https://stanfordvr.com/pubs/2023/misinformation-in-virtual-reality-2/> [accessed 16 June 2023].

34. Daniel Castro, *Content Moderation in Multi-User Immersive Experiences: AR/VR and the Future of Online Speech*, Information Technology & Innovation Foundation, February 2022 <https://itif.org/publications/2022/02/28/content-moderation-multi-user-immersive-experiences-arvr-and-future-online/> [accessed 1 May 2023].

35. Freeman *et al.*, 'Disturbing the Peace'.

36. Rec Room, *Reporting Another Player* (May 2023) <https://recroom.zendesk.com/hc/en-us/articles/4419903977751-Reporting-Another-Player> [accessed 1 June 2023].

37. VR Chat, *I Want to Report Someone* (November 2022) <https://help.vrchat.com/hc/en-us/articles/360062658553-I-want-to-report-someone> [accessed 1 June 2023].

One positive intervention taken by Social VR platforms is the introduction of opt-in safety features for users to stave off harassment themselves. For example, Meta introduced a personal boundary tool for Horizon Worlds after beta testers complained about experiencing virtual sexual harassment.[38]

These affordances are helpful and preventative, and represent a step in the right direction. However, they can only be one piece of a platform content moderation strategy. These tools cannot replace active monitoring and moderation.

Should the metaverse take a decentralised model shape, decentralised metaverse platforms governed by decentralised autonomous organisations (DAOs) may not have the resources to effectively govern and enforce rules at scale in a substantive, coordinated way.

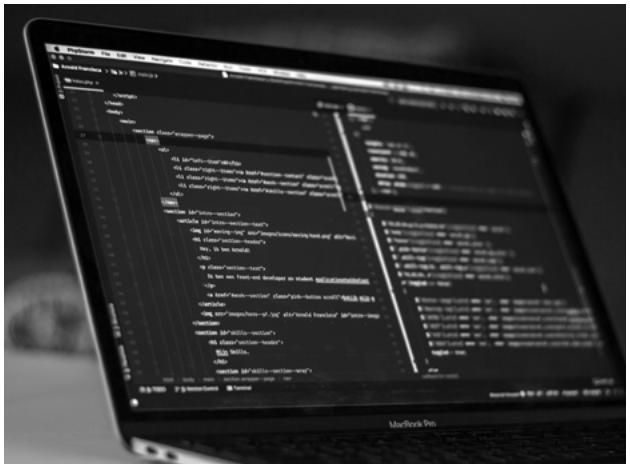
This may present challenges to regulators as there would be no entity that could be held to account for duty of care responsibilities of the Online Safety Bill. Policymakers must consider this possibility and how the legislation will apply in this case.

38. Tanya Basu, 'The Metaverse Has a Groping Problem Already', *MIT Technology Review*, 16 December 2021 <https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/> [accessed 30 March, 2023].

Generative AI Applications in XR

Generative AI will scale content creation in the metaverse. While it is time and labour-intensive to build VR experiences today, the integration of Generative AI in metaverse platforms will speed up the creative process for users.

Social VR platforms are developing Generative AI tools that enable users to use voice or text inputs to instantly generate virtual worlds and objects, as well as design avatars.[39] For example, in 2022, Horizon Worlds showcased a prototype of Builder Bot, a Generative AI tool capable of spawning virtual worlds and objects via voice commands.[40]



Another example, Social VR platform SIMULACRA released an AI tool that allows users to customise their virtual apartments and avatar apparel via text commands.

These features aim to make Social VR platforms more attractive to users and encourage adoption.[41]

Companies must consider how Generative AI tools in XR will be misused to generate illegal content or immersive harmful virtual experiences *en masse*.

For example, Generative AI applications in VR would make it easier to generate and disseminate child sexual abuse material (CSAM) and terrorism content.[42]

Another example, cybersecurity experts have raised alarms about Generative AI's capacity to cheaply produce convincing misinformation in the form of images, video, and audio at scale. Some scholars anticipate that the technology will revolutionise influence operations and disrupt elections.[43]

Pairing Generative AI with XR democratises access to misinformation production tools capable of creating compelling misinformation experiences, or mis-experiences, intended to mislead or confuse audiences at scale.[44]

39. Jeffery Boopathy, 'Real-World Applications of Generative AI in Virtual Reality', *Generative AI*, 5 May 2023 <https://generativeai.pub/real-world-applications-of-generative-ai-in-virtual-reality-6b5109d670f> [accessed 1 June 2023].

40. Aisha Malik, 'Mark Zuckerberg Demos a Tool for Building Virtual Worlds Using Voice Commands', *Tech Crunch*, 23 February 2022 <https://techcrunch.com/2022/02/23/mark-zuckerberg-demos-a-tool-for-building-virtual-worlds-using-voice-commands/> [accessed 24 May 2023].

41. Dominik Kunić, 'SIMULACRA Shows Off First In-Metaverse AI Creator Tools', *Virtualna Stvarnost*, 8 March 2023 <https://virtualnastvarnost.net/en/simulacra-shows-off-first-in-metaverse-ai-creator-tools/> [accessed 25 May 2023].

42. ActiveFence, 'Generative AI is the New Attack Vector for Platforms, According to ActiveFence Threat Intelligence', *Cision PR Newswire*, 23 May 2023 <https://www.prnewswire.com/news-releases/generative-ai-is-the-new-attack-vector-for-platforms-according-to-activefence-threat-intelligence-301831653.html> [accessed 1 June 2023].

43. Josh A. Goldstein *et al.*, 'Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations', *Stanford Internet Observatory*, 10 January 2023, 1–12 <https://arxiv.org/pdf/2301.04246.pdf> [accessed 1 June 2023]; Dan Milmo and Alex Hern, 'Elections in UK and US at Risk from AI-Driven Disinformation, Say Experts', *The Guardian UK*, 20 May 2023 <https://www.theguardian.com/technology/2023/may/20/elections-in-uk-and-us-at-risk-from-ai-driven-disinformation-say-experts> [accessed 25 May 2023].

44. Brown, Bailenson, and Hancock, 'Misinformation in Virtual Reality'.

Child Safety

XR companies do not provide sufficient protection for children in Social VR.

Social VR platforms, which are primarily advertised towards and utilised by children, often fail to to enforce age restrictions and ensure safe, age-appropriate spaces for children. Approximately six per cent of children between the ages of five and ten years old use VR headsets regularly.[45]

Children easily circumvent platform age restrictions by lying about their age or using an older family member's XR device.[46] For example, human moderators in Horizon Worlds do not enforce their 18+ age restriction and remove children who can be easily identified by their voices, instead deferring to the age associated with their Meta accounts.[47]

Social VR platforms are currently falling short of their obligations to perform age verification that would come into force under the Online Safety Bill.[48]

There are little to no barriers for children to access VR social spaces intended for adults. In these largely unmoderated spaces, children can be approached by adults and are exposed to uncensored bullying, sexist and racist hate speech, simulated sexual interactions, and sexual harassment. Conversely, children can harass adults in these spaces as well.

Researchers found that underage users also perpetuate harassment. Children troll adults in Social VR by following them around, screaming or repeating expletives or insults at them, and blocking their view or path till they become frustrated and leave the room.[49]

Due to the lack of consistent monitoring and moderation across Social VR platforms, users often have to manage harassment on their own. Parents are often unaware of available parental monitoring tools, find them overly complex and labour-intensive, and lack the time or interest to activate and monitor them.[50]

Parental monitoring tools do not sufficiently protect children throughout their experiences using VR. Better monitoring and moderation would improve Social VR experiences for everyone.

45. The Institution of Engineering and Technology, *Safeguarding the Metaverse* (IET: 2022) <https://www.theiet.org/media/9836/safeguarding-the-metaverse.pdf> [accessed 1 May 2023].

46. UNICEF Innocenti and Diplo, *The Metaverse, Extended Reality and Children* (UNICEF: Florence, May 2023) <https://www.unicef.org/globalinsight/media/3056/file/UNICEF-Innocenti-Rapid-Analysis-Metaverse-XR-and-children-2023.pdf> [accessed 1 June 2023].

47. SumofUs, *Metaverse*.

48. INEQE Safeguarding Group, *What is Virtual Reality?* <https://ineqe.com/2023/01/10/virtual-reality/> [accessed 1 March 2023].

49. Freeman *et al.*, 'Disturbing the Peace'.

50. Jigsaw Research, *Parents' Views on Parental Controls: Findings of Qualitative Research,* Ofcom, <https://www.ofcom.org.uk/__data/assets/pdf_file/0030/59637/annex_1.pdf> [accessed 10 June 2023]. Stephen Pettifer *et al.*, The Future of eXtended Reality Technologies, and Implications for Online Child Sexual Exploitation and Abuse (University of Manchester, 2022) <https://documents.manchester.ac.uk/display.aspx?DocID=62042> [accessed 16 June 2023].

Case Study: Child Sexual Exploitation in VR

Social VR is shaping up to be a new pathway for online child sexual exploitation. An investigation by ActiveFence observed how child sexual predators and sextortion scammers capitalise on the anonymity and access to children afforded by VR social spaces.

Some tactics used by predatory adults included targeting children based on their voices to elicit sex, drawing children away from other players in lobbies or into private rooms to be alone, and inviting them to continue conversations off-platform on instant messaging apps like Discord.[51]

Adults violated children's personal space by groping their virtual bodies and simulating sex with children's virtual avatars. ActiveFence also found instances of adults attempting to move conversations with minors off-platform or to meet in real life, as well as adults offering money to minors or issuing threats to acquire real photos from children.

Grooming in Social VR can translate to offline exploitation. For example, US authorities arrested a twenty-five-year-old man from Florida after he groomed and kidnapped a thirteen-year-old girl in Utah using VRChat in March 2022. They met virtually and played games together for a month over VRChat until he convinced the child to meet in person.[52]

Metaverse apps exchanging virtual assets may impede the detection of the possession of child sexual abuse material. In 2023, UK authorities discovered eight examples of VR devices being used to store and view CSAM.[53]

51. Stephen Pettifer *et al.*, *The Future of eXtended Reality Technologies, and Implications for Online Child Sexual Exploitation and Abuse* (University of Manchester, 2022) <https://documents.manchester.ac.uk/display.aspx?DocID=62042> [accessed 16 June 2023].

52. Star-Tribune Staff, 'Truck Driver Admits to Transporting 13-Year-Old across State Lines', *Casper Star-Tribune*, 25 October 2022 <https://trib.com/news/state-and-regional/crime-and-courts/truck-driver-admits-to-transporting-13-year-old-across-state-lines/article_d714b906-548e-11ed-b0b8-136167c4f09d.html> [accessed 20 February 2023].

53. Angus Crawford, 'Child Abuse Material Found on VR Headsets, Police Data Shows', *BBC News*, 22 February 2021 <https://www.bbc.co.uk/news/uk-64734308> [accessed 1 May 2023].

Online Safety Bill's Applicability to XR

The proponents of the UK's Online Safety Bill push for the UK to be the safest place in the world to be online. However, the metaverse will challenge any such claim.

The Online Safety Bill establishes responsibilities for platform companies to adequately protect children and adults from encountering illegal content in social media environments. While the legislation does not explicitly address the topic of XR technology and was not drafted with the metaverse in mind, Social VR platforms are liable as user-to-user service providers to its duty of care obligations — particularly to 'mitigate and manage the risks of harm to individuals'.[54]

The Online Safety Bill defines content as 'anything communicated by means of an internet service, whether publicly or privately, including written material or messages, oral communications, photographs, videos, visual images, music and data of any description'.[55]

This definition addresses social media environments, where users publish and passively interact with two-dimensional text, image and video-based content. However, this definition does not encompass the full range of user-to-user interactions and immersive experiences that can take place within XR-enabled virtual environments.[56]

Because the Online Safety Bill was tailored to Web 2.0 internet-based social media applications, some adjustments may be necessary for it to be fully applicable to Web 3.0 metaverse technologies. Under its present definition of 'content', the bill does not provide full coverage for the user-generated content nor user activity possible in metaverse virtual social settings.[57]

An amendment to the Online Safety Bill expanding the definition to address content in the XR medium is necessary to oblige metaverse companies to better protect users from harmful immersive experiences.

54. *Online Safety Bill, as amended in Public Bill Committee* [HC] (Bill 121, 58/3, 28 June 2022) <https://publications.parliament.uk/pa/bills/cbill/58-03/0121/220121.pdf> [accessed 10 May 2023].

55. *Online Safety Bill* [HC] (Bill 121, 58/3, 28 June 2022).

56. The Institution of Engineering and Technology, *Safeguarding the Metaverse*.

57. The Institution of Engineering and Technology, *Safeguarding the Metaverse*.

The definition for content should include:

- User-generated avatar skins and accessories
- Virtual objects
- Virtual rooms and worlds
- Interactive games and activities
- Any user-generated content created using Generative AI

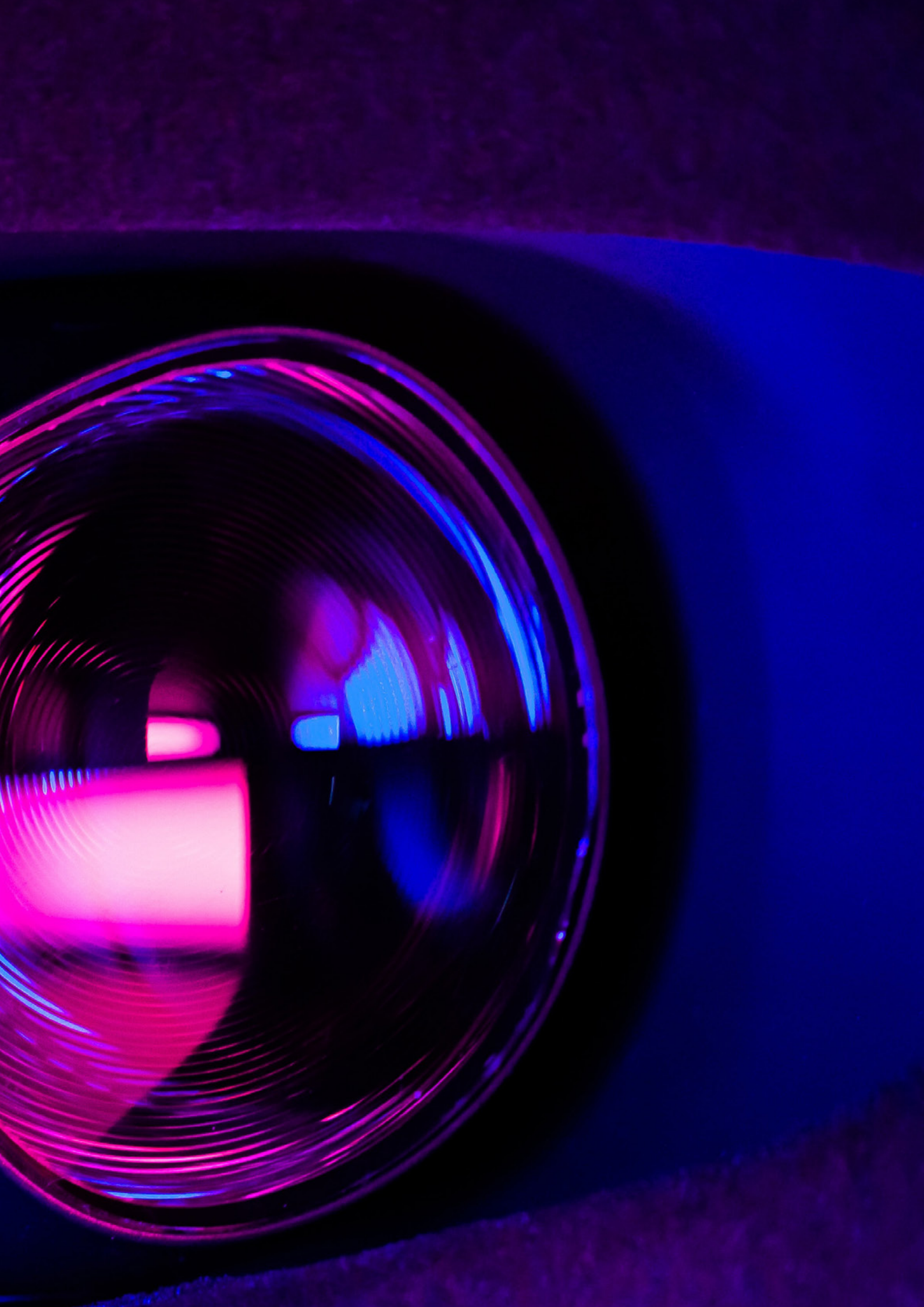
In 2021, Meta's Chief Technology Officer Andrew Bossworth stated publicly that content moderation 'at any meaningful scale is practically impossible' on VR platforms.[58]

While this sentiment speaks to the complexity of preventing harmful behaviour in XR mediums, policymakers cannot allow XR companies to abdicate responsibility for the harms playing out on their platforms, which are largely inhabited by children.

The metaverse needs active monitoring, moderation, and maintenance by the platforms. Human moderation techniques will not be sufficient, given the overwhelming quantity and variety of environments and experiences.

Rather, companies will need to innovate harm-prevention safety features and scalable techniques for monitoring and moderation capable of objurgating on harm and preserving user privacy.

58. Tech Desk, 'Content Moderation in Metaverse "practically impossible": Meta CTO Andrew Bosworth', *The Indian Express*, 16 November 2021 <https://indianexpress.com/article/technology/tech-news-technology/content-moderation-in-metaverse-is-practically-impossible-meta-cto-andrew-bosworth-7625542/> [accessed 15 February 2023].



SECTION II: BIOMETRIC DATA

XR headsets and haptics are an amalgamation of a variety of motion and biosensors. XR devices collect extensive biometric, motion, and environmental data to facilitate convincing, interactive simulations and virtual environments in real-time.

The breadth and intimacy of the biometric data collected by XR devices are hitherto unseen in another consumer-grade product.

XR products on the market today are outfitted with sensors that generate metrics on pupil dilation and reactivity, heart rate, gaze direction, hand and head movements, facial expressions, galvanic skin responses, and some even measure the brain's electrical activity.

Biometric responses tracked throughout gameplay can divulge personal information far beyond what a user would reasonably expect to reveal when putting on an XR headset.

For example, eye-tracking measurements can indicate medical conditions such as ADHD, depression, and personality disorders.[59]

Users may be divulging sensitive information about their health status that they may not yet be aware of.

Additionally, pupil reactivity and skin conductance can reveal information about arousal and sexual orientation.[60]

VR companies have begun utilising these signals to measure headset users' cognitive load while performing virtual tasks[61] as well as their attention level and direction.[62]

59. J. L. Kröger, O. H. M. Lutz, and F. Müller, 'What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking', *Data for Better Living: AI and Privacy*, 576 (2020), 195–208, doi: 10.1007/978-3-030-42504-3_15; Alexandra Voinescu *et al.*, 'The Effectiveness of a Virtual Reality Attention Task to Predict Depression and Anxiety in Comparison with Current Clinical Measures', *Virtual Reality*, 27 (2021), 119–140, doi: 10.1007/s10055-021-00520 7.

60. Chin-An Wang *et al.*, 'Arousal Effects on Pupil Size, Heart Rate, and Skin Conductance in an Emotional Face Task', *Frontiers in Neurology*, 9 (2018), doi: 10.3389/fneur.2018.01029.

61. E. H. Siegel *et al.*, 'HP Omnicept Cognitive Load Database (HPO-CLD) – Developing a Multimodal Inference Engine for Detecting Real-time Mental Workload in VR', *HP Developers*, 30 April 2021 <https://developers.hp.com/omnicept/hp-omnicept-cognitive-load-database-hpo-cld-%E2%80%93-developing-multimodal-inference-engine-detecting-real-time-mental-workload-vr> [accessed 30 April 2023].

62. Demond Cureton, 'Attention Tracking Key to XR Research, CORTEXR Says', *XR Today*, 2 November 2022 <https://www.xrtoday.com/mixed-reality/attention-tracking-key-to-xr-research-cortexr-says-coretxr-says/> [accessed 2 March 2023].

XR-enabled emotion recognition systems are being developed, where machine learning algorithms consider facial expression, vocal inflection, and vital sign data collected by XR headsets to predict users' internal emotional states.[63] These measurements may give XR companies a window into our thoughts, feelings, and desires without our awareness.

XR devices collect the same biosignals as medical devices used in healthcare yet are not held to the same strict regulatory guidelines for processing, deriving diagnostics from, and protecting biometric data.[64]

Such data collection and processing could be ground-breaking for healthcare applications of XR technology. But, for gaming, productivity, or workforce applications, these data present users with more risks than benefits. Such data can present the potential for harms to the user if not properly safeguarded and de-identified.

For example, third parties could make inferences from basic gameplay data to discriminate against people for medical conditions, race, sexual orientation, and other sensitive categories of personal data.

63. Javier Marín-Morales *et al.*, 'Emotion Recognition in Immersive Virtual Reality: from Statistics to Affective Computing', *Sensors*, 20 (2020), 1–26 <https://helios-h2020.eu/wp-content/uploads/2020/11/sensors-20-05163.pdf> [accessed 15 April 2023]; Ekaterina Ivanova and Georgii Borzunov, 'Optimization of Machine Learning Algorithm of Emotion Recognition in Terms of Human Facial Expressions', *Procedia Computer Science*, 169 (2020), 244–248, doi: 10.1016/j.procs.2020.02.143.

64. XR Safety Initiative, *Virtual Worlds: Real Risks and Challenges, 1st XR Data Classification Roundtable Report XR Safety Week 2021 — 10 December 2021* (XRSI, 2022) <https://xrsi.org/wp-content/uploads/2022/02/1st-Data-Classification-Roundtable-Report_v1001.pdf> [accessed 20 February 2023].

User Privacy

It is nearly impossible to de-identify XR data because the body motion data is inherently identifiable.[65] XR devices depend on a constant stream of data about users' physical movements and surroundings to facilitate simulations and translate users' movements into virtual worlds.

Motion data, the most fundamental data stream in XR devices, can compromise a user's identity.[66] Research from the Stanford Virtual Human Interaction Lab shows that body motion data collected in VR can be easily re-identified to individuals after de-identification and is as personally identifiable as a faceprint, fingerprint, or voice print.[67]

In a study from the University of California Berkeley, users were uniquely identified from a pool of over 50,000 people with a 94 per cent accuracy from just 100 seconds of motion data generated playing Beat Saber, the most popular VR game on the market.[68]

This data de-identification problem has profound implications for users' privacy rights and the applicability of privacy laws like the General Data Protection Regulation (GDPR).

Companies may be unable to ensure the de-identification of XR data, which may render corporate adherence to GDPR data de-identification requirements meaningless for XR data.[69]

Motion data may make it impossible for players to remain anonymous in the metaverse.

Another concern is consent. Users cannot reasonably consent to the persistent tracking and monetization of their involuntary biometric responses throughout gameplay. XR companies inadequately inform users about the extent of data capture and processing by XR devices and third-party apps.

Users are unaware of what this sensitive information could potentially reveal about themselves. Moreover, some uses of this data are too complex and opaque for users to provide informed consent for.[70]

Users lack a real choice to 'opt out' of data collection in metaverse technologies, as extensive biometric and biometrically-inferred data is mandatory for XR device functionality.

65. Ellysse Dick, *Balancing User Privacy and Innovation in Augmented and Virtual Reality*, Information Technology & Innovation Foundation, 4 March 2021 <https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/> [accessed 1 April 2023].

66. Mark Roman Miller *et al.*, 'The Effectiveness of a Virtual Reality Attention Task to Predict Depression and Anxiety in Comparison with Current Clinical Measures', *Nature*, 27 (15 October 2020), 1–10, doi: 10.1038/s41598-020-74486 y.

67. Mark Roman Miller *et al.*, 'Personal Identifiability of User Tracking Data during Observation of 360-Degree VR Video', *Scientific Reports*, 10.1 (2020), 17404, doi: 10.1038/s41598-020-74486-y.

68. Viveik Nair *et al.*, 'Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data', 23 February 2023, *arXiv e-prints*, doi: 10.48550/arXiv.2302.08927.

69. Miller *et al.*, 'Personal Identifiability of User Tracking Data'.

70. 'The IEEE Global Initiative on Ethics of Extended Reality (XR) Report — Extended Reality (XR) and the Erosion of Anonymity and Privacy', *Extended Reality (XR) and the Erosion of Anonymity and Privacy — White Paper*, 14 June 2022, 1–31 <https://ieeexplore.ieee.org/document/9794384> [accessed 16 June 2023].

Moreover, users cannot be expected to 'opt out' of XR technology entirely either to protect their individual privacy, as this technology may become a primary conduit for information and content.[71]

Integrating a consent-based model like GDPR to uphold data privacy rights may not work when applied to XR and metaverse technologies. XR may require a different solution to protect user information.

Alternatives to consent-based models that preserve privacy should be considered. Some alternatives include *privacy-by-design*, minimising data collection to only what is necessary to deliver the XR experience, and on-device data processing and storage.[72]

These protocols, while a start, will not solve the metaverse's privacy problems, given that biometric data can indicate identity.

This means that how existing privacy laws apply to XR data is not well-defined. Existing laws do not cover the range of biometric data and biometrically-inferred data categories being collected by XR devices.[73]

XR developers find it difficult to comply with regulations due to their legal ambiguity in relation to XR.Regulators should clarify how existing privacy laws apply to XR products to guide XR companies as they build out XR technology and platforms.[74]

Policymakers should re-evaluate existing privacy laws, such as GDPR, reviewing consent mechanisms and how they apply. Regulators must ensure that privacy laws' definitions for personal data include biometrically-inferred data, as well as encompassing new data types generated by XR systems that could indicate identity — namely, motion and heartbeat data.[75]

Regulators should require companies to engineer *privacy-by-design* to enable the use of XR without exposing personal information, as well as restrict the categories of biometrically inferred data XR companies may share with third-parties.

71. Louis Rosenberg, 'Regulation of the Metaverse: A Roadmap', *6th International Conference on Virtual and Augmented Reality Simulations (ICVARS), 25–27 March, Brisbane, Australia* (2022), 1–10, doi: 10.1145/3546607.3546611.

72. Multiverse, 'Defining the Rules of Data Privacy and Protection in the Metaverse', *Multiverse* <https://www.multiverse.ai/stories/defining-the-rules-of-data-privacy-and-protection-in-the-metaverse> [accessed 1 May 2023].

73. Daniel Berrick and Jameson Spivack, 'Apple is Staffing Up its Ad Business', *Tech Policy Press*, 4 April 2023 <https://techpolicy.press/unpacking-the-privacy-implications-of-extended-reality/> [accessed 1 June 2023].

74. Tooker, Joshua, 'Privacy in the Era of Constant Reality Capture: Informed Consent in Extended Reality (XR)' (unpublished MBA/MSI thesis, University of Michigan, April 2021) <https://deepblue.lib.umich.edu/bitstream/handle/2027.42/168561/20210501_Tooker%2CJoshua_Final_MTOP_Thesis.pdf> [accessed 16 June 2023].

75. Aratek, 'How Heartbeat Biometrics Could be the Next Big Thing?', *Aratek*, 2 February 2023 <https://www.aratek.co/news/how-heartbeat-biometrics-could-be-the-next-big-thing> [accessed 1 May 2023].

Targeted Advertising

The companies investing the most in XR technology are Big Tech giants for whom digital advertising makes up the vast majority of their revenue, or who predict significant gains in advertising revenue in the coming years.

For example, Meta and HTC are introducing AI-generated targeted ads tailored to user interests, inferred from eye-tracking data, in VR.[76]

Another example, Apple announced its first mixed-reality (MR) headset, Vision Pro, in June 2023, and secured patents on XR technology capable of detecting the cognitive state of users — states such as curiosity, fear, attention level, remembering a past experience — and predicting user behaviour based upon biofeedback data from MR devices.[77] Apple doubled the size of its ad business staff in 2022 and is expected to expand its ad business to £24.11 billion by 2026.[78]

This phenomenon is called *biometric psychography*, a concept coined by US attorney Brittan Heller to describe the use of a person's behavioural and anatomical reactions as an 'involuntary like button' to generate insights into their likes, dislikes, preferences, interests, and motives for the purpose of targeted advertising and to recommend relevant content.[79]

Previously only possible in small marketing research lab settings given the extensive biometric sensors required to perform it, XR technology enables neuromarketing research at an unprecedented detail and scale. It can predict consumer behaviour and affinities better than traditional methods of marketing research.[80]

76. Andrew Hutchinson, 'Meta Previews Coming Generative AI Ad Tools, Prompts for VR World Creation', *Social Media Today*, 5 April 2023 <https://www.socialmediatoday.com/news/Meta-Previews-Generative-AI-Ad-Tools/646958/> [accessed 10 April 2023]; Christopher Dring, 'HTC Introduces Eye-Tracking VR Ads', *Games Industry.biz*, 31 March 2017 <https://www.gamesindustry.biz/htc-introduces-eye-tracking-vr-ads> [accessed 1 May 2023]; Hannah Murphy, 'Facebook Patents Reveal How it Intends to Cash in on Metaverse', *Financial Times*, 18 January 2022 <https://www.ft.com/content/76d40aac-034e-4e0b-95eb-c5d34146f647> [accessed 1 April 2023].

77. Crispin Sterling [@sterlingcrispin], 'I spent 10% of my life contributing to the development of the #VisionPro while I worked at Apple as a' [Tweet], *Twitter*, 5 June 2023 <https://twitter.com/sterlingcrispin/status/1665792422914453506> [accessed 16 June 2023].

78. Ryan Barwick, 'Apple is Staffing Up its Ad Business', *Marketing Brew*, 7 September 2022 <https://www.marketingbrew.com/stories/2022/09/07/apple-is-staffing-up-its-ad-business> [accessed 15 May 2023].

79. Avi Bar-Zeev, 'The Eyes Are the Prize: Eye-Tracking Technology Is Advertising's Holy Grail', *VICE*, 28 May 2019 <https://www.vice.com/en_us/article/bj9ygv/the-eyes-are-the-prize-eye-tracking-technology-is-advertisings-holy-grail> [accessed 5 April 2023]; Eben Harrell, 'Neuromarketing: What You Need to Know', *Harvard Business Review*, 23 January 2019, <https://hbr.org/2019/01/neuromarketing-what-you-need-to-know> [accessed 13 February 2023].

80. Harrell, 'Neuromarketing'; Natalia Abuín Vences, Jesús Díaz-Campo, and Daniel Francisco García Rosales, 'Neuromarketing as an Emotional Connection Tool between Organizations and Audiences in Social Networks. A Theoretical Review', *Frontiers in Psychology*, 11 (2020), 1787, doi: 10.3389/fpsyg.2020.01787.

Policymakers must consider how *biometric psychography* techniques in the metaverse may be used to influence or manipulate users' emotions and decision-making. Companies recording XR users' brain activity and emotional responses to elements of virtual experiences without their knowledge or consent, in order to generate insights about users and better target products, is ethically questionable.[81]

Sale and sharing of users' neurological and anatomical response data to third-party entities, such as political campaigning agencies or governments, could be used to influence or manipulate users and worsen existing problems with digital political campaigning.[82]

The use of *biometric psychography* techniques for political advertising could gather insights on voters' neurological responses to candidates and messages and potentially enable customised political campaigns designed to elicit desired reactions.

Biometric psychography paired with Generative AI opens pathways for the creation of highly persuasive and personalised political adverts, disinformation, and influence operations.[83]

An unregulated global trade of XR data could pose a national security risk similar to that of Chinese short-form video app TikTok should XR companies with ties to Beijing fail to handle this data responsibly.

Chinese tech companies are juggernaut competitors in the emerging XR market. For example, Bytedance's Pico is the second most popular VR headset brand on the global market, after Meta's Oculus.[84] Chinese companies Tencent, Baidu, Huawei, SenseTime, OPPO, and Ping An Group are among the world's top ten filers of VR and AR patent applications.[85]

Currently, companies take shelter under the rationale that the data collected is necessary to facilitate convincing virtual simulations and improve product performance. However, XR devices pose a threat to privacy and anonymity online because basic data streams from XR devices are inherently sensitive and cannot be untethered from identity.

Identifying individuals moving throughout the metaverse may create new privacy breaches, such as identity theft or blackmail. If a person's activity in XR, biometric signals, biometrically-inferred qualities, or attention analytics were linked to their real-world identity, there could be consequences for users' privacy, cybersecurity, and personal reputation.

81. Kiran Voleti, 'Political Neuromarketing: How Political Neuromarketing Works?', *Political Marketer*, 16 June 2020 <https://politicalmarketer.com/political-neuromarketing/> [accessed 15 April 2023].

82. Scott Bloomberg, 'Political Advertising in Virtual Reality' (23 February 2023), *First Amendment Law Review*, forthcoming, doi: 10.2139/ssrn.4245908.

83. Bloomberg, 'Political Advertising in Virtual Reality'.

84. IDC, 'Meta's Dominance in the VR Market will be Challenged in the Coming Years, According to IDC', *IDC Corporate*, 30 June 2022 <https://www.idc.com/getdoc.jsp?containerId=prUS49422922> [accessed 20 May 2023] .

85. IDC, 'Meta's Dominance in the VR Market will be Challenged'.

SECTION III: CYBERSECURITY

Policymakers and law enforcement must consider how threat actors will exploit XR and metaverse technologies, as well as urge XR companies to integrate security-by-design into their products.

The extent of data flow within the metaverse, along with this data's diverse applications, pose an escalating risk and expand the cyber attack surface for users. Cybersecurity risks have emerged in the physical hardware of XR devices, as well as within the metaverse's market for non-fungible tokens (NFT) digital assets.

We can expect these vulnerabilities to be exploited if metaverse companies do not resolve them and build in security protocols at the outset to protect users.

Hardware Security

Immense volumes of sensitive data flow through XR devices, making device integrity vital to preserving users' privacy and information security. XR headsets and haptic add-ons must be resilient to malware attacks, distributed denial-of-service (DDoS) attacks, and hacking, as these events may compromise user privacy and open the door to the theft of personal information.

XR headsets contain a wide assortment of motion and biosensors, like other consumer-grade devices, including Internet of Things (IoT) devices.

IoT devices are notorious for having cybersecurity vulnerabilities because they often lack robust security measures.[86] Too often, such devices are not designed with security in mind. They often have inadequate encryption and lack sufficient authentication mechanisms.

It is becoming apparent that XR devices share many of the same cybersecurity gaps that IoT devices have. In 2022, researchers identified cyber vulnerabilities in the motion sensors in the Oculus Quest and HTC VIVE Pro VR headsets.

86. Phillip Williams *et al.*, 'A Survey on Security in Internet of Things with a Focus on the Impact of Emerging Technologies', *Internet of Things*, 29 (2022), 100564, doi: 10.1016/j.iot.2022.100564.

The built-in accelerometer and gyroscope did not require any permission to access, so researchers developed a proof-of-concept eavesdropping attack which enabled them to intercept voice commands and spy on users throughout gameplay and meetings.

Access to speech content could allow people to steal sensitive information communicated by users in voice chat or voice commands, such as passwords and credit card information, potentially leading to user account breaches, digital avatar and identity theft, and fraud.[87]

Fraud

Non-fungible tokens (NFTs) will likely become an important component of the commercialisation of the metaverse. An NFT is a one-of-a-kind cryptographic token recorded on a blockchain representing a virtual item, such as a piece of artwork or virtual real estate.

NFTs are purchased via pseudonymous and irreversible cryptocurrency transactions conducted without intermediaries and with little to no supervision from authorities. Cybercriminals are increasingly using cryptocurrency as a payment medium in organised crime and as investment fraud currency.[88]

The metaverse has attracted a flurry of NFT investors. In 2022, investors spent nearly £1.75 billion in cryptocurrency on virtual land in the metaverse.[89]

Major brand-name companies, like Adidas, Nike, Coca-Cola, McDonald's, and high fashion brands like Gucci and Dolce and Gabbana, have launched NFT ventures.

By opening virtual stores and selling collectable items and avatar apparel, these brands have generated millions in NFT revenue and royalties.[90]

For example, Adidas has generated £8.8 million in NFT sales, plus £3.82 million in royalties. International celebrities like Snoop Dogg and Paris Hilton have purchased virtual land on decentralised Social VR platforms and opened themed virtual worlds for users to meet and buy themed NFT objects and avatar skins in the likeness of the celebrities.[91]

87. Cong Shi *et al.*, 'Face-Mic: Inferring Live Speech and Speaker Identity via Subtle Facial Dynamics Captured by AR/VR Motion Sensors', *MobiCom '21: Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, 25 October 2021, 478–490 doi: 0.1145/3447993.3483272.

88. Europol, Cryptocurrencies: Tracing the Evolution of Criminal Finances, Europol Spotlight, 26 January 2023 <https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf> [accessed 1 March 2023].

89. Joe Tidy, 'Billions Being Spent in Metaverse Land Grab', BBC News, 4 November 2022

90. Florence Muchai, 'List of Brands Selling NFTs in 2023', Cryptopolitan, 14 February 2023 <https://www.cryptopolitan.com/list-of-brands-selling-nfts-in-2023/> [accessed 15 May 2023].

91. Florence Muchai, 'List of Celebrities that Own Land in Metaverse 2023', Cryptopolitan, 16 February 2023 <https://www.cryptopolitan.com/celebrities-that-own-land-in-metaverse-2023/> [accessed 15 May 2023].

However, we are beginning to see this unregulated and unmonitored market be exploited by cybercriminals seeking to profit from investment fraud scams, money laundering schemes, and the exchange of illicit materials.[92]

Five US state law enforcement agencies filed actions against a Russian organisation soliciting American investors and selling fraudulent NFTs in the metaverse casino Flamingo Casino Club.[93]

Phishing websites impersonating official metaverse brands often trick private individual investors into divulging login credentials to their metaverse cryptocurrency wallets, which cybercriminals access and drain of all assets.[94]

With no centralised authority overseeing irreversible transaction processes, users are vulnerable to exploitation without sufficient recourse or support from XR companies and Social VR platforms. Companies offer little to no support for recovering funds when people investing in metaverse assets are robbed, beyond reporting to the authorities.

The metaverse's NFT market is presently a proverbial 'wild west' in dire need of regulation to protect users from attacks from fraudsters and to cut off covert pathways for illegal activity.

XR companies should establish best practices and ethical standards to protect consumers and enhance trust. This should be inclusive of erecting resolution mechanisms and refund policies for NFT transactions, as well as systems for detecting, thwarting, and prosecuting ongoing scams and attacks.

92. Eamon Javers *et al.*, 'Cybercriminals Target Metaverse Investors with Phishing Scams', *CNBC*, 26 May 2022 <https://www.cnbc.com/2022/05/26/cybercriminals-target-metaverse-investors-with-phishing-scams.html> [accessed 19 March 2023] .

93. Texas State Securities Board, 'Five States File Enforcement Actions to Stop Russian Scammers Perpetrating Metaverse Investment Fraud', 11 May 2022 <https://www.ssb.texas.gov/sites/default/files/2022-05/FlamingoPressRelease.pdf> [accessed 19 March 2023].

94. Javers *et al.*, 'Cybercriminals Target Metaverse Investors'.

Abuse of Immersive Learning

XR-enabled immersive learning is revolutionising education and skill training by providing hands-on virtual learning experiences. However, the misuse of XR's immersive learning capabilities by dangerous individuals and organisations poses a national security risk.

XR applications in corporate training have translated to faster learning and improved skills retention.[95] Immersive learning tools train firefighters, pilots, and construction workers for incidents that would be costly or dangerous to recreate. The UK and US militaries use the technology to train soldiers to use equipment and weaponry, develop combat and survival skills in battle scenarios, and deliver battlefield medical treatment.[96]

Immersive learning is a powerful, cost-effective delivery tool for skills training. However, malicious actors may repurpose it in the future to plot and train to commit acts of violence offline. While this is a prospective risk that has yet to manifest, expressions of violent extremism have begun cropping up on metaverse platforms. For example, white supremacists created and circulated video game re-enactments of terrorist attacks by far-right extremists on Social VR platform *Roblox*.[97]

Researchers have discovered first-player shooter games on Roblox that simulated the 2019 Christchurch mosque shootings in New Zealand, the 2019 El Paso mass shooting in the US, and the 2011 car bombing and mass shooting in Utøya, Norway.[98]

Roblox has removed these games and implemented new policies to address this problem. Still, covert links to new versions continue circulating within white supremacist Discord channels and dark web groups.

The Online Safety Bill requires Social VR platforms to monitor and remove illegal terrorism content and swiftly act to secure their platform to prevent further misuse of affordances.

Regulators must ensure that the new XR companies and metaverse platforms entering the mainstream understand their obligations under the law to devote sufficient resources to proactively detecting and removing illegal XR content.

Moreover, regulators should specify precisely what sufficient resources entail in the XR medium.

95. PwC, 'PwC's Study into the Effectiveness of VR for Soft Skills Training', *PwC* <https://www.pwc.co.uk/issues/emerging-technologies/metaverse-technologies/study-into-vr-training-effectiveness.html> [April 18, 2023].

96. Future Visual, 'Uses of VR in Military Training', *FV Future Visual*, <https://www.futurevisual.com/blog/uses-vr-military-training/> [accessed 23 April 2023].

97. Russell Brandom, 'Roblox is Struggling to Moderate Re-Creations of Mass Shootings', *The Verge*, 21 August 2021 <https://www.theverge.com/2021/8/17/22628624/roblox-moderation-trust-and-safety-terrorist-content-christchurch> [accessed 16 June 2023].

98. ActiveFence, *The Exploitation of VR Technologies: ActiveFence Report* <https://www.activefence.com/research/the-exploitation-of-vr-technologies/> [accessed 1 March 2023].

Case Study: Online Extremism & Dangerous Organisations

There is growing concern from US, UK, and EU security agencies about pathways to online radicalisation in online gaming.

While there is no causal link between violent video games and offline violence, there is evidence of right-wing extremist, radical Islamic, and ethnonationalist groups increasingly using online video gaming platforms to target gaming communities to share propaganda, recruit, and mobilise vulnerable youths and young adults.[99]

Social VR platforms provide channels for extremist groups and dangerous organisations to convene, build community, and reinforce in-group beliefs in an immersive way. Violent extremist groups and dangerous organisations may exploit the affordances of Social VR to spread their ideology, recruit, and train a distributed audience on how to commit violence.

Moreover, bad actors may leverage VR technologies to produce and disseminate propaganda material that gamifies and glorifies violence to young audiences.

For example, Roblox hosts ISIS-themed servers where users roleplay as ISIS militants. The servers host first-person shooter game recreations of conflict zones in Iraq and Syria, where users can fight ISIS enemies with other players online.

In February 2023, Singapore's Internal Security Agency detained two teenage boys who became radicalised on the ISIS Roblox servers for engaging in terrorist activities, such as plotting suicide bombings and stabbings.[100]

The young men pledged allegiance to ISIS and roleplayed as ISIS leaders in the server.[101]

99. Suraj Lakhani, *Video Gaming and (Violent) Extremism: an Exploration of the Current Landscape, Trends, and Threats*, European Commission Radicalisation Awareness Network Policy Support (Luxembourg: Publications Office of the European Union, 2021) <https://home-affairs.ec.europa.eu/system/files/2022-02/EUIF%20Technical%20Meeting%20on%20Video%20Gaming%20October%202021%20RAN%20Policy%20Support%20paper_en.pdf> [accessed 22 February 2023].

100. Troughton, James, '16-Year-Old Detained for Playing Multiple ISIS-Themed Roblox Games', *TheGamer*, 22 February 2023 <https://www.thegamer.com/teenager-detained-roblox-isis-themed-servers/> [accessed 22 February 2023].

101. Kimberly Lim, 'Singapore Warns of Radicalisation via Gaming as 2 Teens Issued Orders under ISA Law', *South China Morning Post*, 21 February 2023 <https://www.scmp.com/week-asia/article/3210987/singapore-warns-radicalisation-gaming-2-teens-hit-controversial-isa-law> [accessed 22 February 2023].

SECTION IV: CONCLUSION & RECOMMENDATIONS

XR companies are developing products and platforms where users are insufficiently protected from harm and exploitation.

Users are unable to reasonably consent to the extent of biometric data collection taking place. Social VR platforms and technologies are struggling to enforce their community guidelines and protect users uniformly at scale.

In their current form, Social VR platforms make guaranteeing child safety more difficult and creating welcoming spaces for all more challenging. XR devices gather data that make preserving users' privacy and cybersecurity exceptionally challenging.

We can no longer assume that Big Tech will self-regulate effectively without some level of government oversight.[102] Policymakers should not assume that the XR industry will voluntarily adopt trusted norms that prioritise the safety and privacy of users.

We should not leave the safety of children navigating the metaverse to chance.

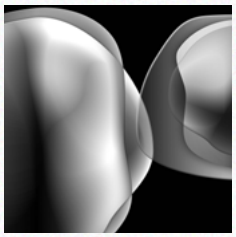
To become resilient and applicable to an XR-enabled future, the UK's Online Safety Bill and other existing privacy laws require re-visiting to specifically address the unique risks inherent in XR technologies and metaverse platforms.

It is vital that regulators be proactive in addressing the risks of XR technologies now, rather than waiting for the harms outlined in this report to affect users *en masse*. Government and industry will need to collaborate now to envision, innovate, and deploy solutions for the future.

Below we outline our recommendations for policymakers and industry to accomplish this.

102. Oxford Internet Institute, 'Press Release: Self-Regulation of Social Media Platforms Failing to Curb Disinformation, Says New Report', *OII News*, 11 October 2019 <https://www.oii.ox.ac.uk/news-events/news/self-regulation-of-social-media-platforms-failing-to-curb-disinformation-says-new-report/> [accessed 15 May 2023]; Paul Karp, 'Digital Code of Conduct Fails to Stop All Harms of Misinformation, Acma Warns', *The Guardian Australia*, 21 March 2022 <https://www.theguardian.com/media/2022/mar/21/digital-code-of-conduct-fails-to-stop-all-harms-of-misinformation-acma-warns> [accessed 10 May 2023].

Recommendations to improve metaverse platform governance:



1. Expand the UK's Online Safety Bill's definition for what qualifies as content with respect to XR

An updated definition of what qualifies as content is needed in the Online Safety Bill to encompass the full range of user-to-user interactions and immersive experiences possible within XR-enabled virtual environments.

The definition for content should include:

- User-generated avatar skins and accessories
- Virtual objects
- Virtual rooms and worlds
- Interactive games and activities
- Any user-generated content created using Generative AI

Regulators should require XR companies to develop effective responses to address intersectional harassment and abuse directed toward women, Black, Asian and minority ethnic (BAME), and other marginalised communities using XR.

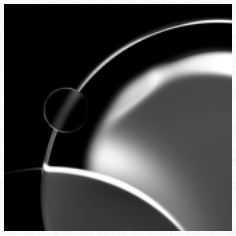
Moreover, Ofcom should encourage XR companies to consider designing in small moments of friction into gameplay that discourage or prevent users from harmful or illegal behaviour and breaking platform rules.[103]

2. Regulators, including the UK's Ofcom, should be proactive about metaverse technologies

Ofcom should be proactive about metaverse technologies and regulators should devote resources and attention to evaluating whether XR companies understand and adequately fulfil their duty of care obligations under the Online Safety Bill, enforce age assurance, and actively monitor for illegal content.

Ofcom should clarify for industry how the Online Safety Bill's definitions for harassment apply in a three-dimensional medium to the behaviours or interactions possible in Social VR.

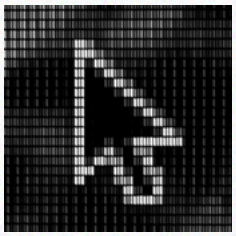
103. Anna L. Cox *et al.*, 'Design Frictions for Mindful Interactions: the Case for Microboundaries', *CHI EA '16: Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, 7 May 2016, 1389–1397, doi: 10.1145/2851581.2892410.



3. Policymakers must establish expectations that companies actively monitor Social VR environments

Policymakers should provide clarification on what the expectations outlined in the Online Safety Bill are for active monitoring and moderation in persistent, live metaverse environments rather than trusting companies to define this for themselves. Policymakers can require companies to adopt content monitoring and hybrid moderation strategies that prioritise safety at scale and reduce the reporting burden placed on people who have experienced abuse. Policymakers also should require Social VR platforms to establish Trust and Safety teams specialising in the XR medium to compose governance policy and moderation strategies tailored to the spatial medium.

Recommendation to protect consumer data in the metaverse:



4. Existing privacy, security and consumer protection laws need to be re-evaluated to ensure that they apply across metaverse devices and experiences

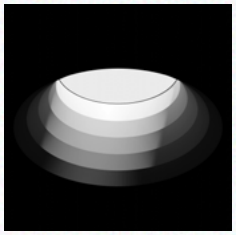
Policymakers must ensure the protection of biometric and biometrically-inferred data generated from XR devices to safeguard human rights to privacy, as well as establish obligations to protect users' cybersecurity. Regulators should also ensure that privacy laws' definitions for personal data encompass the new data types generated by XR systems that may be indicative of identity — namely motion and heartbeat data.

Policymakers should consider expanding the transparency reporting disclosure requirements of the Online Safety Bill to include reporting on data breaches, cyber vulnerabilities in products, incidents of financial fraud related to transactions of virtual assets, and biometric and biometrically-inferred data categories collected. Disclosures should also provide detailed information on data anonymisation procedures and ethical review processes in place before XR user data is shared with third-party entities.

We recommend legislators strengthen existing consumer protection laws to include provisions that specifically cover NFTs and other digital assets in metaverse environments. This could include establishing requirements for platforms to provide clear and accurate information about the NFTs being sold, and creating penalties for fraud and misrepresentation. Federal authorities should be given more powers to tackle the use of Web 3.0 technologies to trade illicit or fraudulent materials.

Companies should adopt robust policies and implement measures that ensure their products and services protect and uphold human rights.

Recommendations to address cybersecurity risks:



5. Governments and industry must commit to embedding security and privacy by design into metaverse products and services

Given the inherent sensitivity of the data collected by XR devices, XR companies must prioritise security-by-design in their products. Regulators should consider incorporating cybersecurity requirements into the duty of care obligations of the Online Safety Bill, ensuring that all hardware and software must be routinely updated with the latest security patches.

Regulators must implore companies to practise privacy-by-design and minimise the amount of personal information they gather. Additionally, lawmakers should re-evaluate consent mechanism requirements and assess their applicability to the XR medium.

Additionally, regulators should ensure that privacy laws' definitions for personal data encompass the new data types generated by XR systems that may be indicative of identity. Regulators should require companies to engineer privacy by design to enable the use of XR without exposing personal information, and as well as restrict the categories of biometrically inferred data XR companies may share with third-parties.

Before the widespread adoption of XR technologies, regulators have a limited window of opportunity to act to ensure its development progresses responsibly and prioritises user safety and privacy.

The regulatory choices we make today can help prevent the entrenchment of harmful metaverse developments that could be difficult, if not impossible, to untangle in the future.

ACKNOWLEDGEMENTS

I am profoundly grateful to the following individuals and organizations for their invaluable contributions and unwavering support throughout the completion of this project.

First and foremost, I would like to express my deepest gratitude to the XR and Trust & Safety industry experts who provided invaluable feedback on the contents of this report: Jeremy Bailenson from Stanford University, Alex Leavitt, and Sam Gilbert from the University of Cambridge's Bennett Institute for Public Policy. Their expertise and insights significantly enriched the quality of this work.

I would like to extend my heartfelt thanks to Gina Neff, Jeremy Hughes, Irene Galandra Cooper, and the entire team at the Minderoo Centre for their generous support, mentorship, and guidance throughout this project. Their expertise and encouragement were instrumental in shaping the direction and scope of my research. Moreover, I am sincerely grateful to the Minderoo Foundation for their support and funding, without which this project would not have been possible.

Special recognition goes to Annie Searle, Dr. Megan Aleah Ward, and especially Dr. Jessica Beyer from the University of Washington. Their nurturing guidance and unwavering support fueled my interest and passion in cybersecurity policy.

I would also like to express my gratitude to Nina Jankowicz and Alexa Pavliuc for their role in cultivating my interests in Trust & Safety. Their mentorship and guidance over the years have been invaluable.

Lastly, I want to extend my deepest appreciation to my family for their unwavering support, encouragement, and belief in me throughout my academic and professional journey.

BIBLIOGRAPHY

ActiveFence, *The Exploitation of VR Technologies: ActiveFence Report* <https://www.activefence.com/research/the-exploitation-of-vr-technologies/> [accessed 1 March 2023]

———, 'Generative AI is the New Attack Vector for Platforms, According to ActiveFence Threat Intelligence', *Cision PR Newswire*, 23 May 2023 <https://www.prnewswire.com/news-releases/generative-ai-is-the-new-attack-vector-for-platforms-according-to-activefence-threat-intelligence-301831653.html> [accessed 1 June 2023]

Adorno, José, 'Apple Execs Reportedly Think Mixed Reality Headset Could Replace the iPhone', *BGR*, 17 April 2023 <https://bgr.com/tech/apple-execs-reportedly-think-mixed-reality-headset-could-replace-the-iphone/> [accessed 1 June 2023]

Aratek, 'How Heartbeat Biometrics Could be the Next Big Thing?', *Aratek*, 2 February 2023 <https://www.aratek.co/news/how-heartbeat-biometrics-could-be-the-next-big-thing> [accessed 1 May 2023]

Bar-Zeev, Avi, 'The Eyes Are the Prize: Eye-Tracking Technology Is Advertising's Holy Grail', *VICE*, 28 May 2019 <https://www.vice.com/en_us/article/bj9ygv/the-eyes-are-the-prize-eye-tracking-technology-is-advertisings-holy-grail> [accessed 5 April 2023]

Basu, Tanya, 'The Metaverse Has a Groping Problem Already', *MIT Technology Review*, 16 December 2021 <https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/> [accessed 30 March, 2023]

Berrick, Daniel, and Jameson Spivack, 'Apple is Staffing Up its Ad Business', *Tech Policy Press*, 4 April 2023 <https://techpolicy.press/unpacking-the-privacy-implications-of-extended-reality/> [accessed 1 June 2023]

Bloomberg, Scott, 'Political Advertising in Virtual Reality' (23 February 2023), *First Amendment Law Review*, forthcoming, doi: 10.2139/ssrn.4245908

Boopathy, Jeffery, 'Real-World Applications of Generative AI in Virtual Reality', *Generative AI*, 5 May 2023 <https://generativeai.pub/real-world-applications-of-generative-ai-in-virtual-reality-6b5109d670f> [accessed 1 June 2023]

Brandom, Russell, 'Roblox is Struggling to Moderate Re-Creations of Mass Shootings', *The Verge*, 21 August 2021 <https://www.theverge.com/2021/8/17/22628624/roblox-moderation-trust-and-safety-terrorist-content-christchurch> [accessed 16 June 2023]

Brown, James G., Jeremy N. Bailenson, and Jeffrey Hancock, 'Misinformation in Virtual Reality', *Journal of Online Trust and Safety*, March 2023 <https://stanfordvr.com/pubs/2023/misinformation-in-virtual-reality-2/> [accessed 16 June 2023]

Castro, Daniel, *Content Moderation in Multi-User Immersive Experiences: AR/VR and the Future of Online Speech*, Information Technology & Innovation Foundation, February 2022 <https://itif.org/publications/2022/02/28/content-moderation-multi-user-immersive-experiences-arvr-and-future-online/> [accessed 1 May 2023]

Cong Shi, Xiangyu Xu, Tianfang Zhang, Payton Walker, Yi Wu, Jian Liu, Nitesh Saxena, Yingying Chen, and Jiadi Yu, 'Face-Mic: Inferring Live Speech and Speaker Identity via Subtle Facial Dynamics Captured by AR/VR Motion Sensors', *MobiCom '21: Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, 25 October 2021, 478–490 doi: 0.1145/3447993.3483272

Barwick, Ryan, 'Apple is Staffing Up its Ad Business', *Marketing Brew*, 7 September 2022 <https://www.marketingbrew.com/stories/2022/09/07/apple-is-staffing-up-its-ad-business> [accessed 15 May 2023]

Chirico, Alice, and Andrea Gaggioli, 'When Virtual Feels Real: Comparing Emotional Responses and Presence in Virtual and Natural Environments', *Cyberpsychology, Behavior, and Social Networking*, 22 (2019), 220–226, doi: 10.1089/cyber.2018.0393

Cox, Anna L., Sandy J. J. Gould, Marta E. Cecchinato, Ioanna Iacovides, and Ian Renfree, 'Design Frictions for Mindful Interactions: the Case for Microboundaries', CHI EA '16: *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, 7 May 2016, 1389–1397, doi: 10.1145/2851581.2892410

Crawford, Angus, 'Child Abuse Material Found on VR Headsets, Police Data Shows', *BBC News*, 22 February 2021 <https://www.bbc.co.uk/news/uk-64734308> [accessed 1 May 2023]

———, and Tony Smith, 'Metaverse App Allows Kids into Virtual Strip Clubs', *BBC News*, 23 February 2022 <https://www.bbc.co.uk/news/technology-60415317> [accessed 12 February 2023]

Cureton, Demond, 'Attention Tracking Key to XR Research, CORTEXR Says', *XR Today*, 2 November 2022 <https://www.xrtoday.com/mixed-reality/attention-tracking-key-to-xr-research-cortexr-says-coretxr-says/> [accessed 2 March 2023]

Danaher, John, 'The Ethics of Virtual Sexual Assault', in *The Oxford Handbook of Digital Ethics*, ed. Carissa Véliz (online edn, Oxford Academic, 10 November 2021), doi: 10.1093/oxfordhb/9780198857815.013.14

Davis, Lee, 'Best Practices for Voice Chat Moderation', *Spectrum Labs*, 29 June 2020 <https://www.spectrumlabsai.com/the-blog/best-practices-for-voice-chat-moderation> [accessed 1 May 2023]

Dick, Ellysse, *Balancing User Privacy and Innovation in Augmented and Virtual Reality*, Information Technology & Innovation Foundation, 4 March 2021 <https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/> [accessed 1 April 2023]

Dring, Christopher, 'HTC Introduces Eye-Tracking VR Ads', *Games Industry.biz*, 31 March 2017 <https://www.gamesindustry.biz/htc-introduces-eye-tracking-vr-ads> [accessed 1 May 2023]

Dwivedi, Yogesh K., Laurie Hughes, Abdullah M. Baabdullah, Samuel Ribiero-Navarrete, Mihalis Giannakis, Mutaz M. Al-Debei, Denis Dennehy, Bhimaraya Metri, Dimitrios Buhalis, Christy M. K. Cheung, Kieran Conboy, Ronan Doyle, Rameshwar Dubey, Vincent Dutot, Reto Felix, D. P. Goyal, Anders Gustafsson, Chris Hinsch, Ikram Jebabli, Marijn Janssen, Young-Gab Kim, Jooyoung Kim, Stefan Koos, David Kreps, Nir Kshetri, Vikram Kumar, Keng-Boon Ooi, Savvas Pagagioannidis, Ilias O. Pappas, Ariana Polyviou, Sang-Min Park, Neeraj Pandey, Maciel M. Quieroz, Ramakrishnan Raman, Philipp A. Rauschnabel, Anuragini Shirish, Marianna Sigala, Konstantina Spanaki, Garry Wei-Han Tan, Manoj Kumar Tiwari, Giampaolo Viglia, and Samuel Fosso Wamba, 'Metaverse Beyond the Hype: Multidisciplinary Perspectives on Emerging Challenges, Opportunities, and Agenda for Research, Practice and Policy', *International Journal of Information Management*, 66 (2022), 102542, doi: 10.1016/j.ijinfomgt.2022.102542 [version of record 16 July 2022]

Europol, *Cryptocurrencies: Tracing the Evolution of Criminal Finances*, Europol Spotlight, 26 January 2023 <https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf> [accessed 1 March 2023]

Fadeev, Kirill A., Alexey S. Smirnov, Olga P. Zhigalova, Polina S. Bazhina, Alexey V. Tumialis, and Kirill S. Golokhvast, 'Too Real to Be Virtual: Autonomic and EEG Responses to Extreme Stress Scenarios in Virtual Reality', *Behavioural Neurology*, 2020 (2020), 1–11, doi: 10.1155/2020/5758038

Federal Trade Commission, 'FTC Seeks to Block Virtual Reality Giant Meta's Acquisition of Popular App Creator Within', *Federal Trade Commission*, 27 July 2022 <https://www.ftc.gov/news-events/news/press-releases/2022/07/ftc-seeks-block-virtual-reality-giant-metas-acquisition-popular-app-creator-within> [accessed 15 April 2023]

Felnhofer, Anna, Oswald D. Kothgassner, Mareike Schmidt, Anna-Katharina Heinzle, Leon Beutl, Helmut Hlavacs, and Ilse Kryspin-Exner, 'Is Virtual Reality Emotionally Arousing? Investigating Five Emotion Inducing Virtual Park Scenarios', *International Journal of Human-Computer Studies*, 82 (2012), 48–56, doi: 10.1016/j.ijhcs.2015.05.004

Freeman, Guo, Samaneh Zamanifard, Divine Maloney, and Dane Acena, 'Disturbing the Peace: Experiencing and Mitigating Emerging Harassment in Social Virtual Reality', *Proceedings of the ACM on Human-Computer Interaction*, 6 (2022), 1–30 <https://dl.acm.org/doi/pdf/10.1145/3512932> [accessed 1 June 2023]

Future Visual, 'Uses of VR in Military Training', *FV Future Visual*, <https://www.futurevisual.com/blog/uses-vr-military-training/> [accessed 23 April 2023]

Gilbert, Sam, 'The Political Economy of the Metaverse', *IFRI: French Institute of International Relations*, Briefings de l'Ifri, 20 June 2022 <https://www.ifri.org/en/publications/briefings-de-lifri/political-economy-metaverse> [accessed 16 June 2023]

Goldstein, Josh A., Girish Sastry, Micah Musser, Renée DiResta, Matthew Gentzel, and Katerina Sedova, 'Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations', *Stanford Internet Observatory*, 10 January 2023, 1–12 <https://arxiv.org/pdf/2301.04246.pdf> [accessed 1 June 2023]

Harrell, Eben, 'Neuromarketing: What You Need to Know', *Harvard Business Review*, 23 January 2019, <https://hbr.org/2019/01/neuromarketing-what-you-need-to-know> [accessed 13 February 2023]

Heath, Alex, 'Meta Opens Up Access to its VR Social Platform Horizon Worlds', *The Verge*, 9 December 2021 <https://www.theverge.com/2021/12/9/22825139/meta-horizon-worlds-access-open-metaverse> [accessed 16 February 2023]

———, 'This is Meta's AR / VR Hardware Roadmap for the Next Four Years', *The Verge*, 1 March 2023 <https://www.theverge.com/2023/2/28/23619730/meta-vr-oculus-ar-glasses-smartwatch-plans> [accessed 10 April 2023]

Heller, Brittan, 'Reimagining Reality: Human Rights and Immersive Technology', *Carr Center for Human Rights Policy*, Harvard Kennedy School, Carr Centre Discussion Paper Series, 2020.008, 12 June 2020 <https://carrcenter.hks.harvard.edu/publications/reimagining-reality-human-rights-and-immersive-technology> [accessed 16 June 2023]

Hutchinson, Andrew, 'Meta Previews Coming Generative AI Ad Tools, Prompts for VR World Creation', *Social Media Today*, 5 April 2023 <https://www.socialmediatoday.com/news/Meta-Previews-Generative-AI-Ad-Tools/646958/> [accessed 10 April 2023]

IDC, 'Meta's Dominance in the VR Market will be Challenged in the Coming Years, According to IDC', *IDC Corporate*, 30 June 2022 <https://www.idc.com/getdoc.jsp?containerId=prUS49422922> [accessed 20 May 2023]

'The IEEE Global Initiative on Ethics of Extended Reality (XR) Report — Extended Reality (XR) and the Erosion of Anonymity and Privacy', *Extended Reality (XR) and the Erosion of Anonymity and Privacy — White Paper*, 14 June 2022, 1–31 <https://ieeexplore.ieee.org/document/9794384> [accessed 16 June 2023]

INEQE Safeguarding Group, *What is Virtual Reality?* <https://ineqe.com/2023/01/10/virtual-reality/> [accessed 1 March 2023]

'Inside the Metaverse: Are You Safe? | Dispatches | Channel 4 Documentaries', *YouTube*, uploaded by Channel 4 Documentaries, 1 October 2022 <https://www.youtube.com/watch?v=ssgLSky8hfg> [26 February 2023]

The Institution of Engineering and Technology, *Safeguarding the Metaverse* (IET: 2022) <https://www.theiet.org/media/9836/safeguarding-the-metaverse.pdf> [accessed 1 May 2023]

Ivanova, Ekaterina, and Georgii Borzunov, 'Optimization of Machine Learning Algorithm of Emotion Recognition in Terms of Human Facial Expressions', *Procedia Computer Science*, 169 (2020), 244–248, doi: 10.1016/j.procs.2020.02.143

Javers, Eamon, Meghna Maharishi, Scott Zamost, and Paige Tortorelli, 'Cybercriminals Target Metaverse Investors with Phishing Scams', *CNBC*, 26 May 2022 <https://www.cnbc.com/2022/05/26/cybercriminals-target-metaverse-investors-with-phishing-scams.html> [accessed 19 March 2023]

Jigsaw Research, *Parents' Views on Parental Controls: Findings of Qualitative Research*, Ofcom, <https://www.ofcom.org.uk/__data/assets/pdf_file/0030/59637/annex_1.pdf> [accessed 10 June 2023]

Karp, Paul, 'Digital Code of Conduct Fails to Stop All Harms of Misinformation, Acma Warns', *The Guardian Australia*, 21 March 2022 <https://www.theguardian.com/media/2022/mar/21/digital-code-of-conduct-fails-to-stop-all-harms-of-misinformation-acma-warns> [accessed 10 May 2023]

Kowert, Rachel, 'Dark Participation in Games', *Frontiers in Psychology*, 11 (2020), doi: 10.3389/fpsyg.2020.598947

Kröger, J. L., O. H. M. Lutz, and F. Müller, 'What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking', *Data for Better Living: AI and Privacy*, 576 (2020), 195–208, doi: 10.1007/978-3-030-42504-3_15

Kunić, Dominik, 'SIMULACRA Shows Off First In-Metaverse AI Creator Tools', *Virtualna Stvarnost*, 8 March 2023 <https://virtualnastvarnost.net/en/simulacra-shows-off-first-in-metaverse-ai-creator-tools/> [accessed 25 May 2023]

Lakhani, Suraj, *Video Gaming and (Violent) Extremism: an Exploration of the Current Landscape, Trends, and Threats*, European Commission Radicalisation Awareness Network Policy Support (Luxembourg: Publications Office of the European Union, 2021) <https://home-affairs.ec.europa.eu/system/files/2022-02/EUIF%20Technical%20Meeting%20on%20Video%20Gaming%20October%202021%20RAN%20Policy%20Support%20paper_en.pdf> [accessed 22 February 2023]

Lim, Kimberly, 'Singapore Warns of Radicalisation via Gaming as 2 Teens Issued Orders under ISA Law', *South China Morning Post*, 21 February 2023 <https://www.scmp.com/week-asia/article/3210987/singapore-warns-radicalisation-gaming-2-teens-hit-controversial-isa-law> [accessed 22 February 2023]

Malik, Aisha, 'Mark Zuckerberg Demos a Tool for Building Virtual Worlds Using Voice Commands', *Tech Crunch*, 23 February 2022 <https://techcrunch.com/2022/02/23/mark-zuckerberg-demos-a-tool-for-building-virtual-worlds-using-voice-commands/> [accessed 24 May 2023]

Marín-Morales, Javier, Carmen Llinares, Jaime Guixeres, and Mariano Alcañiz, 'Emotion Recognition in Immersive Virtual Reality: from Statistics to Affective Computing', *Sensors*, 20 (2020), 1–26 <https://helios-h2020.eu/wp-content/uploads/2020/11/sensors-20-05163.pdf> [accessed 15 April 2023]

McKinsey & Company, Value Creation in the Metaverse: the Real Business of the Virtual World (June 2022) <https://www.mckinsey.com/~/media/mckinsey/business%20functions/marketing%20and%20sales/our%20insights/value%20creation%20in%20the%20metaverse/Value-creation-in-the-metaverse.pdf> [accessed 5 June 2023]

Meta, *Natural Facial Expressions Privacy Notice* (November 2022) <https://www.meta.com/en-gb/help/quest/articles/accounts/privacy-information-and-settings/natural-facial-expressions-privacy-notice/> [accessed 10 March 2023]

Miller, Mark Roman, Fernanda Herrera, Hanseul Jun, James A. Landay, and Jeremy N. Bailenson, 'The Effectiveness of a Virtual Reality Attention Task to Predict Depression and Anxiety in Comparison with Current Clinical Measures', *Nature*, 27 (15 October 2020), 1–10, doi: 10.1038/s41598-020-74486-y

———, 'Personal Identifiability of User Tracking Data during Observation of 360-Degree VR Video', *Scientific Reports*, 10.1 (2020), 17404, doi: 10.1038/s41598-020-74486-y

Milmo, Dan, and Alex Hern, 'Elections in UK and US at Risk from AI-Driven Disinformation, Say Experts', *The Guardian UK*, 20 May 2023 <https://www.theguardian.com/technology/2023/may/20/elections-in-uk-and-us-at-risk-from-ai-driven-disinformation-say-experts> [accessed 25 May 2023]

Muchai, Florence, 'List of Brands Selling NFTs in 2023', *Cryptopolitan*, 14 February 2023 <https://www.cryptopolitan.com/list-of-brands-selling-nfts-in-2023/> [accessed 15 May 2023]

———, 'List of Celebrities that Own Land in Metaverse 2023', *Cryptopolitan*, 16 February 2023 <https://www.cryptopolitan.com/celebrities-that-own-land-in-metaverse-2023/> [accessed 15 May 2023]

Multiverse, 'Defining the Rules of Data Privacy and Protection in the Metaverse', *Multiverse* <https://www.multiverse.ai/stories/defining-the-rules-of-data-privacy-and-protection-in-the-metaverse> [accessed 1 May 2023]

Murphy, Hannah, 'Facebook Patents Reveal How it Intends to Cash in on Metaverse', *Financial Times*, 18 January 2022 <https://www.ft.com/content/76d40aac-034e-4e0b-95eb-c5d34146f647> [accessed 1 April 2023]

Nair, Vivek, Wenbo Guo, Justus Mattern, Rui Wang, James F. O'Brien, Louis Rosenberg, and Dawn Song, 'Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data', 23 February 2023, *arXiv e-prints*, doi: 10.48550/arXiv.2302.08927

Online Safety Bill, as amended in Public Bill Committee [HC] (Bill 121, 58/3, 28 June 2022) <https://publications.parliament.uk/pa/bills/cbill/58-03/0121/220121.pdf> [accessed 10 May 2023]

O'Regan, Sylvia Varnham, and Mathew Olson, 'In Facebook's VR Headset, Racism and Other Abuses Showed Up "Like Clockwork"', *The Information*, 12 November 2021 <https://www.theinformation.com/articles/in-facebooks-vr-headset-racism-and-other-abuses-showed-up-like-clockwork> [accessed 10 March 2023]

Oxford Internet Institute, 'Press Release: Self-Regulation of Social Media Platforms Failing to Curb Disinformation, Says New Report', *OII News*, 11 October 2019 <https://www.oii.ox.ac.uk/news-events/news/self-regulation-of-social-media-platforms-failing-to-curb-disinformation-says-new-report/> [accessed 15 May 2023]

Pettifer, Stephen, Emma Barrett, James Marsh, Kathryn Hill, Polly Turner, and Sandra Flynn, *The Future of eXtended Reality Technologies, and Implications for Online Child Sexual Exploitation and Abuse* (University of Manchester, 2022) <https://documents.manchester.ac.uk/display.aspx?DocID=62042> [accessed 16 June 2023]

Pluta, Agnieszka, Joanna Mazurek, Jakub Wojciechowski, Tomasz Wolak , Wiktor Soral, and Michał Bilewicz, 'Exposure to Hate Speech Deteriorates Neurocognitive Mechanisms of the Ability to Understand Others' Pain', *Scientific Reports*, 13 (2023), 1–12, doi: 10.1038/s41598-023-31146-1

Porter, Michael E., and James E. Heppelmann, 'Why Every Organization Needs an Augmented Reality Strategy', *Harvard Business Review*, Nov–Dec 2017, 46–57 <https://hbr.org/2017/11/why-every-organization-needs-an-augmented-reality-strategy> [accessed 6 February 2020]

PwC, 'PwC's Study into the Effectiveness of VR for Soft Skills Training', *PwC* <https://www.pwc.co.uk/issues/emerging-technologies/metaverse-technologies/study-into-vr-training-effectiveness.html> [April 18, 2023]

Rec Room, *Reporting Another Player* (May 2023) <https://recroom.zendesk.com/hc/en-us/articles/4419903977751-Reporting-Another-Player> [accessed 1 June 2023]

Ritterbusch, Georg David, and Malte Rolf Teichmann, 'Defining the Metaverse: A Systematic Literature Review', *IEEE Access*, 11 (2023), 12368–12377, doi: 10.1109/ACCESS.2023.3241809

Rosenberg, Louis, 'Regulation of the Metaverse: A Roadmap', *6th International Conference on Virtual and Augmented Reality Simulations (ICVARS)*, 25–27 March, Brisbane, Australia (2022), 1–10, doi: 10.1145/3546607.3546611

Siegel, E. H., J. Wei, A. Gomes, M. Oliviera, P. Sundaramoorthy, K. Smathers, M. Vankipuram, S. Ghosh, H. Horii, J. Bailenson, and R. Ballagas, 'HP Omnicept Cognitive Load Database (HPO-CLD) – Developing a Multimodal Inference Engine for Detecting Real-time Mental Workload in VR', *HP Developers*, 30 April 2021 <https://developers.hp.com/omnicept/hp-omnicept-cognitive-load-database-hpo-cld-%E2%80%93-developing-multimodal-inference-engine-detecting-real-time-mental-workload-vr> [accessed 30 April 2023]

Sobieraj, Sarah, *Credible Threat: Attacks against Women Online and the Future of Democracy* (Oxford: Oxford University Press, 2020), doi: 10.1093/oso/9780190089283.001.0001

Söderlund, Otto, 'Why Games Need Better Voice Chat Moderation', *Speechly*, 24 October 2022 <https://www.speechly.com/blog/why-games-need-better-voice-chat-moderation> [accessed 15 May 2023]

———, 'Voice Chat is Popular with Gamers — It's also the Top Source of Toxic Behavior — New Report', *Speechly*, 8 March 2023 <https://www.speechly.com/blog/voice-chat-is-popular-with-gamers-its-also-the-top-source-of-toxic-behavior-new-report> [accessed 15 May 2023]

Star-Tribune Staff, 'Truck Driver Admits to Transporting 13-Year-Old across State Lines', *Casper Star-Tribune*, 25 October 2022 <https://trib.com/news/state-and-regional/crime-and-courts/truck-driver-admits-to-transporting-13-year-old-across-state-lines/article_d714b906-548e-11ed-b0b8-136167c4f09d.html> [accessed 20 February 2023]

Sterling, Crispin [@sterlingcrispin], 'I spent 10% of my life contributing to the development of the #VisionPro while I worked at Apple as a' [Tweet], *Twitter*, 5 June 2023 <https://twitter.com/sterlingcrispin/status/1665792422914453506> [accessed 16 June 2023]

SumofUs, *Metaverse: Another Cesspool of Toxic Content* (May 2022) <https://www.eko.org/images/Metaverse_report_May_2022.pdf> [accessed 10 February 2023]

Takahashi, Dean, 'Modulate's ToxMod Uses AI to Scan Game Voice Chat for Toxic Speech', *Venture Beat*, 14 December 2020 <https://venturebeat.com/business/modulates-toxmod-uses-ai-to-scan-game-voice-chat-for-toxic-speech/> [accessed 23 February 2023]

Tall, Tidjane, 'Augmented Reality vs Virtual Reality vs Mixed Reality', *Toptal*, 21 September 2021, <https://www.toptal.com/designers/ui/augmented-reality-vs-virtual-reality-vs-mixed-reality> [accessed March 4 2023]

Tech Desk, 'Content Moderation in Metaverse "practically impossible": Meta CTO Andrew Bosworth', *The Indian Express*, 16 November 2021 <https://indianexpress.com/article/technology/tech-news-technology/content-moderation-in-metaverse-is-practically-impossible-meta-cto-andrew-bosworth-7625542/> [accessed 15 February 2023]

Texas State Securities Board, 'Five States File Enforcement Actions to Stop Russian Scammers Perpetrating Metaverse Investment Fraud', 11 May 2022 <https://www.ssb.texas.gov/sites/default/files/2022-05/FlamingoPressRelease.pdf> [accessed 19 March 2023]

Tidy, Joe, 'Billions Being Spent in Metaverse Land Grab', *BBC News*, 4 November 2022 <https://www.bbc.co.uk/news/technology-63488059> [accessed 10 May 2023]

Tooker, Joshua, 'Privacy in the Era of Constant Reality Capture: Informed Consent in Extended Reality (XR)' (unpublished MBA/MSI thesis, University of Michigan, April 2021) <https://deepblue.lib.umich.edu/bitstream/handle/2027.42/168561/20210501_Tooker%2CJoshua_Final_MTOP_Thesis.pdf> [accessed 16 June 2023]

Tremosa, Laia, 'Beyond AR vs. VR: What is the Difference between AR vs. MR vs. VR vs. XR?', *Interaction Design Foundation*, 2022 <https://www.interaction-design.org/literature/article/beyond-ar-vs-vr-what-is-the-difference-between-ar-vs-mr-vs-vr-vs-xr> [accessed 20 January 2023]

Troughton, James, '16-Year-Old Detained for Playing Multiple ISIS-Themed Roblox Games', *TheGamer*, 22 February 2023 <https://www.thegamer.com/teenager-detained-roblox-isis-themed-servers/> [accessed 22 February 2023]

UNICEF Innocenti and Diplo, *The Metaverse, Extended Reality and Children* (UNICEF: Florence, May 2023) <https://www.unicef.org/globalinsight/media/3056/file/UNICEF-Innocenti-Rapid-Analysis-Metaverse-XR-and-children-2023.pdf> [accessed 1 June 2023]

Vences, Natalia Abuín, Jesús Díaz-Campo, and Daniel Francisco García Rosales, 'Neuromarketing as an Emotional Connection Tool between Organizations and Audiences in Social Networks. A Theoretical Review', *Frontiers in Psychology*, 11 (2020), 1787, doi: 10.3389/fpsyg.2020.01787

Verhulsdonck, Tijmen, Dario Kneubuhler, Inaki Navarro Oiza, Ian Sachs, and Kiran Bhat, 'Real Time Facial Animation for Avatars', *Roblox*, 22 March 2022 <https://blog.roblox.com/2022/03/real-time-facial-animation-avatars/> [accessed 10 March 2023]

Voinescu, Alexandra, Karin Petrini, Danaë Stanton Fraser, Radu Adrian Lazarovicz, Ion Papavă, Liviu Andrei Fodor, and Daniel David, 'The Effectiveness of a Virtual Reality Attention Task to Predict Depression and Anxiety in Comparison with Current Clinical Measures', *Virtual Reality*, 27 (2021), 119–140, doi: 10.1007/s10055-021-00520-7

Voleti, Kiran, 'Political Neuromarketing: How Political Neuromarketing Works?', *Political Marketer*, 16 June 2020 <https://politicalmarketer.com/political-neuromarketing/> [accessed 15 April 2023]

VR Chat, *I Want to Report Someone* (November 2022) <https://help.vrchat.com/hc/en-us/articles/360062658553-I-want-to-report-someone> [accessed 1 June 2023]

Wang, Chin-An, Talia Baird, Jeff Huang, Jonathan D. Coutinho, Donald C. Brien, and Douglas P. Munoz, 'Arousal Effects on Pupil Size, Heart Rate, and Skin Conductance in an Emotional Face Task', *Frontiers in Neurology,* 9 (2018), doi: 10.3389/fneur.2018.01029

Williams, Phillip, Indira Kaylan Dutta, Hisham Daoud, and Magdy Bayoumi, 'A Survey on Security in Internet of Things with a Focus on the Impact of Emerging Technologies', *Internet of Things*, 29 (2022), 100564, doi: 10.1016/j.iot.2022.100564

XR Safety Initiative, *Virtual Worlds: Real Risks and Challenges, 1st XR Data Classification Roundtable Report XR Safety Week 2021 — 10 December 2021* (XRSI, 2022) <https://xrsi.org/wp-content/uploads/2022/02/1st-Data-Classification-Roundtable-Report_v1001.pdf> [accessed 20 February 2023]

Yousefi, Midia, and Dimitra Emmanouilidou, 'Audio-Based Toxic Language Classification Using Self-Attentive Convolutional Neural Network', *29th European Signal Processing Conference (EUSIPICO)* (August 2021), doi: 10.23919/EUSIPCO54536.2021.9616001

MINDEROO

CENTRE FOR TECHNOLOGY & DEMOCRACY

Alison Richard Building
7 West Road, Cambridge
CB3 9DT

www.mctd.ac.uk

minderoo@crassh.cam.ac.uk

UNIVERSITY OF CAMBRIDGE

Report design by **CHRIS PRINTED THIS**

Images taken from Unsplash and Pexels courtesy of: Arnold Fransisca, Arthur Edelmans, Daniel Olah, Dmitry Chernyshov, Ernest Ojeh, Giu Vicente, Haidan, Ian Battaglia, James Yarema, Jeshoots.com, Jesper Aggergaard, Jocelyn Morales, Jure Tufekcic, Kaitlyn Baker, Kenny Eliason, Luke Jones, Markus Spiske, Maxim Hopman, Maxim, Tolchinskiy, Mediamodifier, Milad Fakurian, Remy Gieling, Shubham Dhage, Simon Lee, Stella Jacob, Thomas Lefebvre, Towfiqu Barbhuiya, Ugur Akdemir, Umberto, XR Expo