

Across the metaverse: Policy priorities

An essay submitted to the IIC Competition for Future Leaders



July 2022

Abstract

The metaverse and use of immersive technologies dominate conversation around the future of the social internet and of society. Excitement around the metaverse is well-placed; this immersive, interconnected landscape could transform the way we socialise, entertain ourselves and work.

This paper argues that, while the metaverse provides a fertile ground for innovation, regulators can learn lessons from the commercial and consumer harms experienced on social media and in the online games that form proto-metaverses.

These harms could abound on the metaverse without regulation around interoperability, digital assets, data, reporting and child protection.

Failure to understand how harms on social media could be replicated and even exacerbated by the immersive nature of the metaverse could risk financial, commercial and societal consequences.

Introduction

In April 2018, Mark Zuckerberg, CEO of Facebook¹ faced questioning from US senators over the Cambridge Analytica scandal, in which nearly 90 million users had their data shared without their knowledge.²

84-year-old Senator Orrin Hatch asked, “So, how do you sustain a business model in which users don’t pay for your service?”.

“Senator, we run ads”, Zuckerberg said, smiling.³

By then, Facebook’s annual revenue was nearly \$56 billion, and it had 2.2 billion monthly active users.⁴ It had already acquired both Instagram and WhatsApp. While the world came to terms with the power held by Big Tech, the Facebook horse had not only bolted but was settled in a beach-front ranch, counting its billions.

The Collingridge Dilemma says that in the early stages of the emergence of a new technology, when it would be relatively easy to shape its development, it is difficult to know the impact it will have. However, once the technology develops and the ethical and social effects are understood, it is harder to influence.⁵ This fine line between ensuring safe growth and encouraging innovation is well-known to regulators.

While the metaverse may seem far off, the gaming industry has already established virtual worlds where users engage in socialisation and commerce. These ‘proto-metaverses’ should act as a canary in the coalmine for the issues that may be faced with the metaverse.

Lessons learnt from social media and proto-metaverses could provide policymakers with both a warning signal and a blueprint for the importance of early-stage regulation.

Consumers and markets were hurt by largely unregulated global platforms when it came to traditional social media and the metaverse presents an opportunity to avoid history repeating itself.

¹ Facebook rebranded as Meta in late 2021.

² [Facebook says 87 million people’s data was taken in the Cambridge Analytica scandal – far more than previously thought](#), Insider, April 2018

³ [Mark Zuckerberg testifies on Capitol Hill \(full Senate hearing\)](#), Washington Post on YouTube, April 2018

⁴ [Facebook revenue and usage statistics \(2022\)](#), BusinessofApps, June 2022

⁵ [How to Shape a Better Future? Epistemic Difficulties for Ethical Assessment and Anticipatory Governance of Emerging Technologies.](#), Mittelstadt, Brent Daniel, et al., Ethical Theory and Moral Practice, vol. 18, no. 5, November 2015

Commercial policy issues

The social internet tends towards a 'winner takes most' market structure and this has led to the dominance of a few major players, such as Meta, Google and Twitter. Walled-garden platforms cause users to flock towards larger platforms in order to be able to communicate with the largest number of people. The metaverse could see this same network effect, allowing a few market players to dominate. However, interoperability could reduce the threat of oligopoly.

In addition, the creative economy opened up by the metaverse presents both an opportunity and a risk for amateur developers.

Interoperability

In the early days of mobile, users were charged less to call people on their same network, due to call termination charges. This created a financial incentive to remain on the same network as regular contacts, even if there were other incentives to switch. A reduction in these charges lowered the impact on consumers and allowed them to choose a phone contract based on suitability, rather than on the behaviour of others, and encouraged switching.

The metaverse, like the social internet and those early days of mobile, could create a similar network effect for consumers – incentivising them to choose a platform based on popularity rather than suitability. Interoperability could therefore prove critical to the freedom of users to choose.

Interoperability, which in this case would rely on open standards, promises a borderless experience as users migrate between worlds and platforms, taking with them their data, identity and digital assets.

There are, however, some issues with this vision as technology currently stands. The building of virtual worlds requires complex gaming engines to design their physical attributes. These engines each use their own coding and virtual laws of physics to enable movement, design and interactive features. Even when using the same engine, designers make choices that individualise their games and make the transfer of assets difficult. Moving a digital item between two games, whether they are hosted on the same or different engines, would take significant reworking. This doesn't make interoperability impossible, but it does make it difficult, especially without standardisation.

A metaverse hosted entirely on one platform or created using one consistent engine may solve this problem. For example, Horizon Worlds hosts different user-generated worlds

within its platform, but the creative tools are consistent so users can move between them seamlessly. However, this would require a level of monopoly which users and policymakers may not tolerate.

Even if there were several large walled-garden metaverses, this could create a lock-in effect: a user who has invested in assets on one metaverse may not feel able to switch to another if this meant a loss of financially or personally valuable assets and/or social isolation.

Alternatively, interoperability could be achieved if a large enough group of stakeholders agreed to a set of open standards to align creations in the metaverse. An attempt to reach this consensus has already begun, with the launch of the Metaverse Standards Forum in June 2022 of which notable members include Meta, Microsoft, and Nvidia.⁶

This approach would create common technical standards to be used by any platform wishing to be part of the interoperable metaverse, in theory allowing assets and data to be ported between them.

Although it is arguable that standardisation could impede innovation, interoperability in this sense could also be beneficial for knowledge-sharing during the development phase and would ultimately give users freedom to move between platforms, supporting a healthy, competitive market.

Regulation is only necessary if there is not sufficient market incentive to standardise and this newly created standards forum is a step towards standardisation without regulatory burden.

User-generated content and remuneration

A metaverse would likely rely on a marketplace of creations, designed by professional developers, users or both. The willingness of amateur developers to contribute to this space can be harnessed to unlock innovative content. However, while this commerce of digital assets could open up a new strand of economy, there are some risks with regard to compensation.

Proto-metaverse Roblox has received criticism in this regard. The platform allows users to craft 'experiences' on the platform using its design tools and has encouraged users to monetise these, insinuating that large amounts of money could be made.⁷ However, Roblox reportedly takes a 75% cut from sales and pays its creators in Robux, its in-game currency.⁸

⁶ [Metaverse Standards Forum](#)

⁷ [Investigation: How Roblox is exploiting young game developers](#), People Make Games on YouTube, August 2021

⁸ ['Roblox' is allegedly exploiting young game developers](#), NME, August 2021

Users can exchange this currency for regular currency but, to do so, they must first earn 50,000 Robux and submit a tax form.⁹

It is not clear how future metaverse hosts might remunerate developers. However, reliance on user-generated content could fail if creators do not feel fairly compensated for their work. There is an opportunity for regulation to ensure that creators are remunerated in a currency that they can use freely.

There are also questions around how intellectual property rights will be ensured and copyright will be enforced in the metaverse, when content is being created and shared quickly and without active moderation. Brands have already begun to create content for proto-metaverses, and platforms may need to set up protections to scan for copyright infringement or counterfeit digital assets.

⁹ [Developer Exchange \(DevEx\) FAQs](#), Roblox

Consumer harms

Social media and online gaming platforms have each gained significant media attention for harms faced by their users, from mishandling of user data to the proliferation of damaging and illegal content.

The immersive nature of the metaverse could entrench these issues, with virtual reality (VR) and augmented reality (AR) headsets collecting vast amounts of highly personal data and users facing harm in new ways.

Biometric data collection

Big Tech has faced scandals over the collection, use and sale of user data. The introduction of immersive technologies further complicates this.

VR/AR headsets are capable of collecting a huge amount of biometric data, tracking a person's body, voice and eye movements. Just five minutes' use of a VR headset collects enough data to identify a person with 95% accuracy.¹⁰

Microsoft's AR headset, HoloLens 2, tracks a user's eye movements and Microsoft lists one of the potential applications for such data as allowing "commercial companies to perform marketing and consumer studies in real-world environments."¹¹ Meta has also begun to patent technology to track eye, face and body movements¹² and has said that data could be used to inform advertisers of users' attention.¹³

Biometric data, where used for identification purposes, is classed as special category under the General Data Protection Regulations, meaning it can only be processed under certain conditions (i.e. with explicit consent).¹⁴

If the metaverse and immersive technologies gather large amounts of data, including biometric data, platforms must be explicit about how it is being used and users should be allowed to opt out of any use that goes beyond the functionality of the platform.

A study has shown that eye tracking data can contain cues to a user's gender, age, ethnicity, moods and emotions, and physical and mental health condition.¹⁵ This is significant

¹⁰ [Personal identifiability of user tracking data during observation of 360-degree VR video](#), Miller, M.R., Herrera, F., Jun, H. et al., Sci Rep 10, 17404, 2020

¹¹ [Eye tracking on HoloLens 2](#), Microsoft, April 2022

¹² [Meta is looking into eye-tracking and product placement to make money in the metaverse](#), Protocol, January 2022

¹³ [Facebook patents reveal how it intends to cash in on the metaverse](#), Financial Times, January 2022

¹⁴ [Special category data](#), Information Commissioner's Office

¹⁵ [What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking](#), Kröger, J.L., Lutz, O.H.M., Müller, F., Privacy and Identity Management. Data for Better Living: AI and Privacy,

especially as concerns have been raised about how GDPR protects personal data that is inferred rather than known, for example if data suggests to a certain degree of accuracy that someone is suffering a particular health condition without express confirmation of this fact.¹⁶

The collection of data is important in the early stages of development of new technologies. However, user privacy should be a key consideration for platforms and regulators. The huge amount of data conferred when using immersive technologies changes the data protection landscape significantly.

Regulators could ensure that providers are complying with GDPR from the off and consider the additional harm to consumers if this sensitive or inferred data is mishandled.

Reporting and redress

The Online Safety Bill proposes to ensure that platforms have easy-to-use reporting functions for users.¹⁷ These can be used to report both illegal content on all services and content that is considered legal but harmful on some.

Government debates around the metaverse suggest that this Bill should be future-proofed in such a way to capture metaverse technologies.¹⁸ The real-world impacts of illegal and harmful content, such as the exploitation of children and the proliferation of hate speech mean that harmful content on the metaverse must be tackled. Proto-metaverses have already seen harmful content on their platforms and delay in the application of this regulation could have online and real-world consequences.

Regulation could ensure that platforms allow users to report content quickly and easily to either the software platform or the hardware provider and these should have appropriate redress mechanisms.

It is worthwhile, however, noting what makes these metaverses different to traditional social platforms. Namely, the majority of content is being created in real time, is ephemeral and is contained in semi-closed worlds. As such, regulations that apply to traditional social media platforms may need to be extended to take account of this dimension of harm.

Privacy and Identity 2019. IFIP Advances in Information and Communication Technology, vol 576, March 2020

¹⁶ [A right to reasonable inferences: Rethinking Data Protection Law in the age of Big Data and AI](#), Sandra Wachter, Brent Mittelstadt, Oxford Business Law Blog, October 2018

¹⁷ [The Online Safety Bill](#), 17(1-5), July 2022

¹⁸ In the [Lords Chamber debate on online sexual harassment of children](#), volume 818, January 2022, Lord Parkinson of Whitley Bay says, “the online safety Bill takes the approach of not being specific on certain technologies and making sure that our legislation can be future-proofed so that, as the internet continues to develop and new technologies are invented, the legislative protections for users keep pace with that. The metaverse [...] is a key example.”

Often on metaverse-style platforms, people are brought together based on their choice of 'world'. This presents two main issues: contact mapping and retention of data.

Contact mapping is already established in gaming. For example, a player on Fortnite who wishes to report another can access a list of recently encountered users in order to identify them in a retroactive report.¹⁹ It could be required that metaverse platforms keep contact logs, allowing a person to review whom they have encountered and retroactively report behaviour that contravenes community guidelines.

A record of the verbal and visual content of these interactions may also be necessary. Given that communication on these platforms is, for the mostly part, not publicly recorded, it will be important that the platform can review interactions retrospectively.

Sony's PlayStation voice chat function records a rolling five-minute section of communication so that users can select and submit a forty second clip of their recent interactions for review, directly through the PlayStation console.²⁰

A regulatory requirement on platforms or hardware providers to hold a similar rolling log of interactions could facilitate reporting. However, the question remains as to how long platforms should be required to store this information. Recording each interaction in the metaverse and holding it indefinitely on the device or cloud is not feasible, due to data storage limitations. However, if a user removes themselves from the experience or waits a period of time before reporting, they may lose access to redress mechanisms.

Robust reporting mechanisms allow users to protect themselves from harm and there is an opportunity here for platforms to consider preventing the passage of time from being an inhibitor to reporting.

Embodiment of harm

The UK's upcoming Online Safety Bill says that content can be harmful due to, amongst other things, "the manner of its dissemination".²¹ It is critical to consider this in the context of the metaverse, whose dissemination will likely be via immersive technologies.

Regulation could ensure that the effect of immersion within a harmful experience is considered. A person using a VR/AR headset may feel physically threatened by someone, even in a virtual environment. For example, there have already been reported instances of groping in the metaverse.²²

¹⁹ [How to report bad player behaviour in Fortnite](#), Epic Games

²⁰ [Details on new voice chat functionality coming to PS5](#), PlayStation.Blog, October 2020

²¹ [The Online Safety Bill](#), 190(3)(c), July 2022

²² [The metaverse has a groping problem already](#), MIT Technology Review, December 2021

It is not yet clear how harmful virtual forms of physical intimidation can be and opinions on this kind of incident vary.²³ However, there is significant enough concern that Meta has already put in place protections in Horizon Worlds, such as the ‘Safe Zone’,²⁴ which temporarily removes a user from their virtual environment, and a default four-foot ‘personal boundary’ between avatars who are not ‘friends’ on the platform.²⁵

Regulators now have the opportunity to work with platforms to understand how virtualised physical assault and intimidation affect users of immersive technologies and the metaverse. Guidelines on physical safety features and community guidelines relating to physical conduct to prevent intimidation should also be considered.

Child protection

Most social media sites have a minimum age requirement of 13 years. However, 90% of children aged 11-12 use one or more of these age-restricted services.²⁶ This statistic, coupled with the fact that children are often early adopters of new technologies and are already skilled users of proto-metaverses, means that child safety should be a regulatory priority in the metaverse.

There have already been instances of age-inappropriate content on proto-metaverse platforms. Roblox, which is reportedly used by two thirds of all children between the ages of nine and 12 in the US²⁷, has seen users create virtual strip clubs and simulate sex with each other.²⁸ There have also been reports of users wearing digitally created Nazi uniforms.²⁹

Though easy access to age-inappropriate content is an internet-wide issue, the immersive nature of the metaverse, as well as the use of an avatar as an extension of one’s identity, could make these instances more psychologically harmful.

It could be argued that there are two solutions to the issue of children in the metaverse: keep them out or keep them separate.

However, both of these are fundamentally flawed. Stringent age-verification may certainly be an aim for policymakers, but this is yet to have been successfully achieved on traditional social platforms and could create obstacles to access for those who are not digitally literate.

²³ [From ‘silly’ to ‘scumbag’: Reddit discussion of a case of groping in a virtual reality game](#), Lucy A. Sparrow, University of Melbourne, 2020

²⁴ [What is the Safe Zone in Horizon Worlds?](#), Meta

²⁵ [Introducing a personal boundary for horizon worlds and venues](#), Oculus blog, February 2022

²⁶ [New research into underage use of social media sites](#), Childwise, February 2019

²⁷ [Roblox: the children’s game with a sex problem](#), BBC News, February 2022

²⁸ [Inside the underground strip-club scene on kid-friendly gaming site Roblox](#), RollingStone, September 2021

²⁹ [Roblox: the children’s game with a sex problem](#), BBC News, February 2022

The alternative solution could be to create spaces that are age-appropriate for children, ensuring that they are protected from harm. Club Penguin, a virtual world created for children aged between eight and 14, for example, had strict language controls and a large number of human moderators.³⁰ However, scaling this up to a potential metaverse, with myriad different interactive worlds happening simultaneously, could be difficult.

Expecting that children can be completely excluded from the use of immersive technologies or the metaverse is unrealistic. Instead, regulators or platforms could enforce, at a base level, a minimum age to access these platforms, with the expectation on platforms to ensure the age verification of their users in a robust fashion that does not digitally exclude any other user.

The ICO's Age-Appropriate Design Code³¹ helpfully sets out guidance on the protection of children on online services. Its application to the metaverse could ensure that there is a high level of privacy for all users on platforms where there may be child users and that the data collected from children is carefully mapped.

On platforms where there are likely to be child users, a mix of human and non-human content moderation to review age-inappropriate content and behaviour may be favourable, with underage users blocked from accessing this content.

In addition, platforms could be required to proactively seek out and screen spaces targeted at children, more closely monitoring the design, content and interactions in those spaces.

³⁰ [C-c-c-click on clubpenguin](#), Independent.ie, January 2007

³¹ [Age appropriate design: a code of practice for online services](#), ICO

Conclusion

Innovation around the metaverse has the potential to contribute to the economy, democratise experiences and enhance our social and working lives.

However, as social media platforms were allowed to grow mostly without regulation, we have seen retrospective attempts to stem the proliferation of harmful content and anti-trust cases brought against big tech companies.

The metaverse should be considered an opportunity to build platforms with fair market structures and consumer protection as their fundamental foundation. Rather than considering this to be burdensome, collaboration between platforms and regulators could help to ensure that users feel safe and are able to trust platforms with their most sensitive data. The compensation of developers for their work and the protection of their intellectual property rights, could help to build a fairer creative economy.

The metaverse is an opportunity to transform society and our interactions with each other. But it is also an opportunity for regulators to work with platforms to learn from the past and build safer spaces for users.