Vilnius University

European Master's Programme in Human Rights and Democratisation
A.Y. 2021/2022

The Legal Ramifications of Virtual Harms:
A Study into the Human Rights Implications of a Meta-led Metaverse

Author: Lisa Dolan
Supervisor: Dr. Paulius Jurčys

Abstract

Big Tech is hailing the metaverse as the next evolution of the internet. Facebook, having rebranded as Meta in October 2021, is one of the driving forces behind this new digital frontier and will play a leading role in shaping its trajectory. However, the term ‘metaverse’ is rooted in dystopian fiction and has no precise definition, thus, it is little understood by the general public and scholars alike. Moreover, Meta has been the subject of widespread criticism for its failure to prevent the proliferation of hate speech and disinformation resulting in real-world harms. This has fostered scepticism over the company’s attempts to establish dominion over the metaverse and sparked broader concerns about how human rights will continue to be protected in such extended reality environments. Therefore, this paper explores how the right to privacy and data protection and women and children’s rights will be implicated by the company’s metaverse ambitions. The legal issues arising from this analysis are also examined along with their potential remedies. These legal issues are approached from a specifically European perspective by relying upon EU legislation and the case law of the Council of Europe as the legal mechanisms devised by these institutions will likely set the global standard for metaverse regulation in the future. Finally, this paper proposes a set of recommendations for metaverse governance to help guarantee human rights will continue to be respected and protected in this new digital realm.

Acknowledgements

Firstly, I wish to thank my supervisor Dr. Paulius Jurčys for his invaluable support and guidance throughout the thesis-writing process and his enthusiasm for the topic. Thank you also to the academic team at the Global Campus of Human Rights for not only providing academic expertise but also emotional support during the second semester period.

Secondly, I am grateful to my fellow colleagues whom I have met on the EMA programme for always offering great feedback and moral support during group thesis writing sessions.

Lastly, I would like to thank my family, particularly my parents, who have motivated me and shown me great patience and kindness over these past months.

List of Abbreviations

California Consumer Protection Act	CCPA
Brain Computer Interface	BCI
European Data Protection Board	EDPB
Google, Apple, Facebook, and Amazon	GAFA
General Data Protection Regulation	GDPR
Group of Experts on Action against Violence against Women and Domestic Violence	GREVIO
Non-fungible Token	NFT
UN Guiding Principles on Business & Human Rights	UNGPs
User experience/ User interface	UX/UI

Table of Contents

List of Figures

Introduction

Tech evangelists are hailing the metaverse to be the next evolution of the Internet.[1] Some even predict that within the next decade, the alternate digital universes we are accustomed to seeing in dystopian movies such as Ready Player One or Avatar will become a reality.[2] While the development of such innovative technologies is justifiably accompanied by great praise and excitement for the future, many scholars continue to express concern about how human rights will be protected in this new digital realm.[3] International human rights law is slow to evolve and has only recently begun to acknowledge the extension of human rights to digital spaces. However, technology is already moving well beyond this by creating fully immersive mixed reality worlds that pose unforeseen challenges to human rights protection.

The past six months have seen many 'big players' of the tech industry begin to invest heavily in metaverse-related technologies. For example, Microsoft is attempting to acquire video game development company Activision Blizzard for USD 68.7 billion,[4] meanwhile, Sony and Kirkbi have pledged to invest USD 2 billion in Epic Games, the company behind Fortnite.[5] However, this paper is limited to a discussion on the developments happening at Meta (formerly Facebook) for several reasons. First, Meta is the largest social networking company which means that its activities have wide-ranging impacts on global society. In 2021, the company generated a total revenue of USD 117.93 billion and reported having 2.9 billion active monthly users across all Facebook-owned platforms.[6] In addition to this, unlike some companies' nebulous ambitions for the future, Meta has presented a clear vision for the metaverse and a staunch determination to transform this vision into reality. In October of 2021, the company

[1] 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 27 March 2022.
[2] Alex Heath, 'Mark Zuckerberg on Why Facebook Is Rebranding to Meta' *The Verge* (28 October 2021) <https://www.theverge.com/22749919/mark-zuckerberg-facebook-meta-company-rebrand> accessed 18 June 2022.
[3] Katitza Rodriguez and others, 'Virtual Worlds, Real People: Human Rights in the Metaverse' *Electronic Frontier Foundation, Access Now* (9 December 2021) <https://www.eff.org/deeplinks/2021/12/virtual-worlds-real-people-human-rights-metaverse> accessed 18 June 2022.
[4] Sarah Frier and Dina Bass, 'Microsoft Makes a $69 Billion Down Payment on the Metaverse' *Bloomberg* (19 January 2022) <https://www.bloomberg.com/news/articles/2022-01-19/microsoft-msft-activision-blizzard-atvi-deal-shows-big-tech-metaverse-push> accessed 16 April 2022.
[5] Ryan Browne, 'Sony and the Lego Family Bet Big on the "metaverse" with $2 Billion Investment in Epic Games' *CNBC* (11 April 2022) <https://www.cnbc.com/2022/04/11/sony-and-lego-family-invest-2-billion-in-fortnite-creator-epic-games.html> accessed 11 April 2022.
[6] Meta Platforms, Inc., 'Meta Reports Fourth Quarter and Full Year 2021 Results' (2 February 2022) <https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx> accessed 19 June 2022.

famously rebranded to 'Meta' which signified an important shift in the company's focus away from social networking and towards the development of augmented and virtual reality hardware.[7] Zuckerberg has already invested USD 10 billion into Facebook Reality Labs, the division of the company spearheading its metaverse transition with the help of world-class engineers, developers, and researchers.[8] In this way, Meta has secured a first-mover advantage in staking its claim on shaping the trajectory of the future.

However, to date Meta has also been embroiled in countless scandals involving the proliferation of hate speech, disinformation, and censorship online, which Amnesty International claims is linked to the company's 'surveillance-based business model predicated on human rights abuse.'[9] These harms have been felt globally and have resulted in real-world violence, instability, and democratic backsliding.[10] Moreover, in May of 2022, a proposal by investors and advocacy groups to conduct a third-party assessment into the potential human rights harms caused by the metaverse was voted down by Meta's shareholders, of whom Zuckerberg possesses the controlling vote.[11] Hence, a discussion around the human rights implications of Zuckerberg's metaverse is not only timely but necessary to prevent widespread violations of human rights caused by the unregulated use of these powerful new technologies. It will be the task of future research to build upon this analysis and to cover more companies that are moving into the metaverse space.

Hence, this paper explores the human rights implications of a Meta-led metaverse. The aim of the study is twofold: (a) to identify the changes that need to be made to existing legislation in response to the new challenges posed by these innovative technologies and (b) to propose a set of considerations for regulators in order to guarantee that human rights continue to be respected in a Meta-led metaverse. Therefore, this work is guided by the following research questions: (1) How will human rights be impacted by Meta's new technologies? (2) What are the legal

---

[7] Meta, 'The Metaverse and How We'll Build It Together -- Connect 2021' (28 October 2021) 1:14:30 <https://youtu.be/Uvufun6xer8?t=1> accessed 27 March 2022..

[8] Jacob Kastrenakes, 'Facebook Is Spending at Least $10 Billion This Year on Its Metaverse Division' *The Verge* (25 October 2021) <https://www.theverge.com/2021/10/25/22745381/facebook-reality-labs-10-billion-metaverse> accessed 18 April 2022.

[9] 'The Facebook Papers: What Do They Mean from a Human Rights Perspective?' *Amnesty International* (4 November 2021) <https://www.amnesty.org/en/latest/campaigns/2021/11/the-facebook-papers-what-do-they-mean-from-a-human-rights-perspective/> accessed 21 May 2022.

[10] Dan Milmo, 'Rohingya Sue Facebook for £150bn over Myanmar Genocide' *The Guardian* (6 December 2021) <https://www.theguardian.com/technology/2021/dec/06/rohingya-sue-facebook-myanmar-genocide-us-uk-legal-action-social-media-violence> accessed 21 May 2022.

[11] Meta Platforms, Inc., Notice of Annual Meeting & Proxy Statement (2022) <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/22a38320-0a0a-4f62-935d-41ab580273de.pdf> accessed 21 May 2022.

loopholes that these human rights implications expose in existing legislation? (3) What considerations should regulators take into account when regulating for a human rights-compliant metaverse in the future? This paper approaches these questions from the perspective of European legal norms set by the EU and the Council of Europe. European states tend to be more interventionist when it comes to regulating big tech, as evidenced by the European Parliament's recent adoption of the Digital Services Package.[12] Therefore, the legislative mechanisms devised by these institutions to regulate the metaverse will likely set the global standard, thus, providing a solid basis for this analysis to be built upon.

This study employs a qualitative case-study approach in order to answer the research questions defined above. The case study design allows for in-depth analysis from various viewpoints into the potential human rights implications of Meta's new hardware. This helps to avoid the uncertainty and ambiguity associated with exploratory studies of under-researched and little-understood phenomena, such as the metaverse.[13] It also provides a valuable opportunity for this novel topic to be studied within its specific historical context.[14] A combination of inductive and deductive reasoning then permits evidence-based generalisations to be made about the broader impacts of similar technologies and recommendations for the future to be derived from the analysed data.[15] Throughout the study, an empirical and systematic approach to data analysis is used to ensure the study remains grounded in objectivity and to guarantee that subsequent findings are reliable and valid.[16]

Owing to the novelty of the topic there is a general lack of academic literature on this subject. Therefore, this paper is an early contributor to what is hoped to be an emerging field in academic research. To date, few studies have investigated the legal issues associated specifically with Zuckerberg's metaverse technologies. For example, Brittan Heller's 'Reimagining Reality: Human Rights and Immersive Technology' makes no mention of the

[12] European Parliament, Digital Services: landmark rules adopted for a safer, open online environment' (5 July 2022) <https://www.europarl.europa.eu/news/en/press-room/20220701IPR34364/digital-services-landmark-rules-adopted-for-a-safer-open-online-environment> accessed 7 July 2022.
[13] Yazdan Mansourian, 'Exploratory Nature of, and Uncertainty Tolerance in, Qualitative Research' (2008) 109 New Library World 273, 284.
[14] Pamela Baxter and Susan Jack, 'Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers' (2015) 13(4) The Qualitative Report, 544 <https://nsuworks.nova.edu/tqr/vol13/iss4/2/> accessed 19 June 2022.
[15] Mansourian (n 13) 284.
[16] Melissa P. Johnston, 'Secondary Data Analysis: A Method of which the Time Has Come' (May 2017) 3(3) Qualitative and Quantitative Methods in Libraries 619, 620 <http://www.qqml-journal.net/index.php/qqml/article/view/169> accessed 19 June 2022.

metaverse and refers more broadly to the impact of emerging immersive technologies.[17] Thus, this paper takes a different approach by providing a contextual analysis of the metaverse and tailored recommendations for its governance. Furthermore, while Egliston and Carter (2021) do write specifically about Meta, albeit from a critical data studies perspective, they focus only on Oculus Quest, Meta's virtual reality technology.[18] This renders my in-depth discussion on Codec Avatars from multiple human rights perspectives particularly novel for the field.

In order to address the research questions in a logically consistent way, this paper has been divided into four themed chapters. In the first chapter, I define the metaverse as it is understood throughout this study. A comparative analysis of existing theories on the subject is used to arrive at this definition. Then, the metaverse is placed within the historical context of the evolution of the internet. Furthermore, the technologies currently under development at Facebook Reality Labs are detailed to provide a basis for analysis in the following chapters. The second chapter focuses on the right to privacy and data protection. In particular, it considers the legal and socio-ethical implications of using biometric data to build Codec Avatars. It also highlights the potential for encroachment upon freedom of thought in the context of new metaverse technologies that rely upon the collection of sensitive neural data. The third chapter examines the pervasive issue of sexual harassment of women and children in social virtual reality. From the perspective of photorealistic Codec Avatars, this warrants a brief elaboration on the proteus effect and the phenomenon of avatar ownership in immersive reality environments. This leads to a discussion on the attempts of platforms to regulate the behaviour of users and questions about how criminal and civil law can apply to cases of sexual harassment in the metaverse. Finally, the fourth chapter leverages the findings of the previous chapters to develop four key elements that policymakers should take into account when regulating the metaverse of the future: (1) consider the economic incentives at play; (2) mandate the prioritisation of UX/UI design; (3) rectify the identified legal issues, and (4) consider the broader socio-ethical implications. These four practical considerations are designed to ensure the regulatory and legal environment remains well-informed and supportive of innovation yet capable of preventing abuses of human rights.

[17] Brittan Heller, 'Reimagining Reality: Human Rights and Immersive Technology' (Carr Center Discussion Paper Series 2020).
[18] Ben Egliston and Marcus Carter, 'Critical questions for Facebook's virtual reality: data, power and the metaverse' (2021) 10(4) Internet Policy Review <https://doi.org/10.14763/2021.4.1610> accessed 18 April 2022.

Chapter 1: The Metaverse: Its Origins, Characteristics, and Wider Context

As an emerging concept, opinions differ among experts as to the parameters that define the metaverse and whether it already exists.[19] Therefore, before proceeding, it is necessary to clarify precisely what is meant by the 'metaverse' within the scope of this research paper. This facilitates the positioning of Meta's technologies within the broader context of the metaverse and Web 3.0, which will aid the identification of potential human rights implications that are specific to Meta's vision for the future.

In light of this, the following chapter provides an overview of the technological, historical, and legislative context of the metaverse. First, it defines what the metaverse is by describing three of its foundational characteristics – hardware, interoperability, and decentralisation. A brief overview of Web 1.0, Web 2.0, and Web 3.0 then serves to highlight the important regulatory framework that has emerged to govern Web 2.0. Finally, this chapter details the specific metaverse technologies under development at Facebook Reality Labs that will be the focus of subsequent chapters.

The Characteristics of the Metaverse

As it stands, there is no consensus on the definition of the metaverse. Interestingly, the term has dystopian origins as Neal Stephenson was the first to use it in his 1992 sci-fi novel *Snow Crash.* Stephenson employed the term to describe a fictional 3D digital world accessible through VR goggles that allowed users to escape a violent and poverty-stricken America run by corrupt corporate entities.[20] The novel highlights many important themes, such as the perils of gig work, screen addiction, and corporate power, that are even more relevant three decades later.[21] However, beyond any possible parallels with today's society, Stephenson's depiction of a lawless simulated world that encourages users to indulge their darkest desires is a rather extreme version of the metaverse we are likely to experience in the coming years or decades. Considering this, Matthew Ball, who has written prolifically about the subject, has highlighted the futility of contriving a definition for a metaverse that does not yet exist.[22] Instead, he

[19] Cathy Hackl, 'Defining The Metaverse Today' *Forbes* (2 May 2021) <https://www.forbes.com/sites/cathyhackl/2021/05/02/defining-the-metaverse-today/> accessed 20 June 2022.
[20] Brian Merchant, 'The Metaverse Has Always Been a Dystopian Idea' *Vice* (30 July 2021). <https://www.vice.com/en/article/v7eqbb/the-metaverse-has-always-been-a-dystopia> accessed 21 May 2022.
[21] Neal Stephenson, *Snow Crash* (Penguin 1992).
[22] Matthew Ball, 'The Metaverse: What It Is, Where to Find It, and Who Will Build It' *MatthewBall.vc* (13 January 2020) <https://www.matthewball.vc/all/themetaverse> accessed 26 March 2022.

recommends focusing on several different aspects that it is certain to possess, which will be discussed below.

Hardware

Firstly, extended reality (XR) is the foundational idea that underpins the metaverse. XR refers to the combination of augmented reality (AR), virtual reality (VR), and mixed reality (MR) technologies to create an immersive experience that blurs the distinction between the real and the simulated world.[23] Evidently, creating such an immersive and realistic experience that blends fluidly with the physical world will require cutting-edge hardware, such as VR headsets, AR glasses, haptic gloves, biosensors, and tracking devices, all working in conjunction with software.[24] These immersive devices will give the user the impression that they are truly 'in' the metaverse. This is the key difference between the metaverse and the internet. While users of the internet can read and create content on the World Wide Web, metaverse users will be fully immersed in it. Hence why Mark Zuckerberg himself has often referred to the metaverse as an 'embodied internet.'[25]

Interoperability

Fortnite and Roblox are examples of independent virtual worlds that already exist. Players can access these platforms through VR headsets or AR apps for a more immersive experience. Fortnite has also built a strong sense of social connection among its users by organising events such as virtual concerts, which go far beyond the scope of traditional video games.[26] Horizon is set to be Meta's version of a virtual world in the metaverse. Although the platform mainly focuses on building social VR experiences it will soon be accessible on mobile devices without the need for an Oculus VR headset.[27] However, no matter how technologically advanced or socially complex these independent virtual worlds become, the metaverse cannot be said to

[23] 'Extended Reality (XR)' *Electronic Frontier Foundation* <https://www.eff.org/issues/xr> accessed 21 April 2022.
[24] Matthew Ball, 'Hardware and the Metaverse' MatthewBall.vc (29 June 2021) <https://www.matthewball.vc/all/hardwaremetaverse> accessed 21 May 2022.
[25] Casey Newton, 'Mark Zuckerberg Is Betting Facebook's Future on the Metaverse' *The Verge* (22 July 2021) <https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview> accessed 26 March 2022.
[26] Michael Barbaro, 'Microsoft and the Metaverse' *The New York Times* (20 January 2022) 06.30 <https://www.nytimes.com/2022/01/20/podcasts/the-daily/metaverse-microsoft-activision-blizzard.html> accessed 19 April 2022.
[27] Jay Peters, 'Meta Is Working on a Web Version of Its Horizon Worlds Metaverse Platform' *The Verge* (14 April 2022) <https://www.theverge.com/2022/4/14/23025899/meta-horizon-worlds-web-version-metaverse-platform> accessed 22 June 2022.

exist until they are interconnected, allowing users and objects to move easily between them.[28] Akin to the internet which consists of a network of web-based services, the metaverse can be thought of as 'an integrated network of 3D worlds.'[29] Interoperability will not only allow users and their avatars to teleport between worlds in the metaverse, but this cross-platform compatibility will also apply to digital assets, economies, systems, and communication.[30] For example, if a user purchases a digital asset in one virtual marketplace it should always be accessible to them even when visiting other metaverse worlds. Furthermore, Microsoft Vice Executive Charlie Bell has highlighted the importance of interoperability for guaranteeing user security in the metaverse. In a recent company blog post he wrote that 'trust cannot end at the doorway of a virtual meeting space.'[31] Therefore, common safety and security standards must be integrated into the metaverse from the outset.

Interoperability also poses the largest engineering challenge to the creation of a metaverse which is why it has not been realized yet. Zuckerberg has said that teleporting between worlds and platforms in the metaverse should be as easy as clicking a link on the internet.[32] However, existing virtual worlds such as Fortnite and Roblox have, thus far, been unable to render this kind of interconnectedness. This would require all the relevant stakeholders to agree on a common coding language, shared open standards, and an overarching mode of governance.[33] While recent initiatives like the Metaverse Standards Forum[34] attempt to do just that there is a lack of business incentive for companies to allow avatars and digital assets that are bought and monetized on other platforms to operate in their own platform.[35] This could explain why Meta

[28] K.Nevelsteen, 'Metaverse Interoperability Keynote (with Slides and Annotation) AIBC UAE 2022' (5 May 2022) 04.25 <https://www.youtube.com/watch?v=3dxrAvjaqf8> accessed 22 May 2022.
[29] John David N. Dionisio, William G. Burns III, and Richard Gilbert, '3D Virtual worlds and the metaverse: Current status and future possibilities' (2013) 45(3) ACM Computing Surveys 1 <http://dx.doi.org/10.1145/2480741.2480751> accessed 22 June 2022.
[30] Ball (n 22).
[31] Charlie Bell, 'The Metaverse Is Coming. Here Are the Cornerstones for Securing It.' *The Official Microsoft Blog* (28 March 2022) <https://blogs.microsoft.com/blog/2022/03/28/the-metaverse-is-coming-here-are-the-cornerstones-for-securing-it/> accessed 21 May 2022.
[32] Meta (n 7) 07.55.
[33] Edd Gent, 'Q&A: Why the Metaverse Needs to Be Open' *IEEE Spectrum* (18 August 2021) <https://spectrum.ieee.org/open-metaverse> accessed 19 April 2022.
[34] Metaverse Standards Forum, 'Leading Standards Organizations and Companies Unite to Drive Open Metaverse Interoperability' (12 May 2022) <https://metaverse-standards.org/news/press-releases/leading-standards-organizations-and-companies-unite-to-drive-open-metaverse-interoperability/> accessed 21 June 2022.
[35] Todd Harris, 'The Muddled Metaverse - A Case against NFT Interoperability in Videogames.' *LinkedIn* (1 January 2022) <https://www.linkedin.com/pulse/muddled-metaverse-case-against-nft-interoperability-todd-harris/> accessed 21 June 2022.

is choosing to focus the majority of its investment on the development of metaverse hardware as opposed to assuming the sole duty of creating an interoperable metaverse ecosystem.

Decentralisation

The idea of the metaverse is an inherently decentralised one. According to Kim Nevelsteen, users will be able to create and have control over their own virtual worlds in the metaverse, similar to buying and registering a web domain on the internet.[36] As mentioned above, this will require consensus among stakeholders when it comes to the coding language used and the common standards and principles integrated into this decentralised system of systems.[37] Epic Games CEO and proponent of the open metaverse, Tim Sweeney, has said the metaverse cannot be built or owned by one sole company, akin to the way no one company or government owns the internet.[38] Decentralisation will also ensure the metaverse is persistent and ubiquitous, meaning it will continue to change and develop even when the user is logged off.[39] In this sense, the growing Web 3.0 trends of decentralised finance and NFTs built upon distributed blockchain technology will make up the key infrastructure of the metaverse.

However, a distinction must be made here between two emerging visions for virtual worlds within the metaverse. On the one hand, many writers propose that open, decentralised worlds based on the principles of user-centricity and ownership are the only viable options for the future.[40] Examples of existing decentralised platforms include Somnium Space, Decentraland, and Vircadia. However, corporations like Meta will likely attempt to create closed, or 'walled garden', virtual worlds in order to extract the most monetary value from the metaverse.[41] While Zuckerberg has recognised the need for open standards and interoperability to build an integrated system of virtual worlds, experts have pointed out that the company's centralized infrastructure and practice of trading user data for marketing purposes are incompatible with decentralisation.[42] Thus, Meta's business model requires one ruling authority to gather user data and store it on a centralized database for further processing, which places power solely in

[36] Nevelsteen (n 28) 05.55.
[37] ibid, 06:35.
[38] Andrew Hayward, '"No Company Can Own" the Metaverse, Says Epic Games CEO' Decrypt (17 November 2021) <https://decrypt.co/86323/no-company-can-own-metaverse-epic-games-ceo-tim-sweeney> accessed 22 May 2022.
[39] Ball (n 22).
[40] Justin Sun, 'Why the Future of the Metaverse Can Only Be Decentralized' VentureBeat (5 March 2022) <https://venturebeat.com/2022/03/05/why-the-future-of-the-metaverse-can-only-be-decentralized/> accessed 22 May 2022.
[41] ibid.
[42] Jamie Burke, '>The Open Metaverse OS_' (January 2021) 8 <https://outlierventures.io/wp-content/uploads/2021/08/OV-Metaverse-OS_V6.pdf> accessed 17 April 2022.

the hands of the company. In turn, the user has limited control over their decisions, rules, and data when availing of Meta's products and services.[43] However, as journalist Kevin Roose points out, we are likely to end up with a metaverse that contains both open and closed virtual worlds built by different actors with varying preferences.[44]

In short, the metaverse can be understood, not only as a successor to the internet, but also as a digital replica of the real world that will require its own economy, governing structure, and its own legal framework. This chapter has determined that the metaverse does not exist yet, however, this affords regulators some time to get to grips with emerging technologies and develop feasible solutions for their governance. The analysis provided below will aid this process by delving deeper into Meta's vision for the future. Regardless of where the company's metaverse falls on the spectrum of closed and open platforms, it will have major implications for human rights.

A Brief History of the Evolution of the Internet: Web 1.0 through to Web 3.0

The internet has developed in stages often referred to as Web 1.0, Web 2.0, and Web 3.0. Web 1.0 was the earliest version of the Internet that came about in the 1990s. Based on the principle of open source and with the aim of giving users unprecedented access to all sorts of reading materials, Web 1.0 is said to have 'heralded the democratisation of information.'[45] It is also referred to as the 'read-only' internet because it only consisted of web pages with simple text.[46] Web 2.0 is the iteration of the internet we currently have which is much more interactive than Web 1.0. Thus, we can say that the internet evolved from 'read only' to 'read and write.' Not only can users read content, but they can also generate it.[47] Web 2.0 has also benefitted from the development of cloud-based technologies and servers that can store this data, often referred to as big data. This has led to the rise of social media and, subsequently, large technology corporations that have established centralised monopolies over user data.[48] Web 3.0 is the next evolution of the internet that will encompass the creation of the metaverse. It has been referred

[43] ibid, 21.
[44] Michael Barbaro (n 26) 12:30.
[45] 'Web3, the Metaverse, and the Future of the Internet' *Verdict* (17 March 2022) <https://www.verdict.co.uk/web3-metaverse-internet/> accessed 22 April 2022.
[46] Kuntal Chakraborty, 'What Is Web 1.0? - Definition from Techopedia' *Techopedia.com* (29 June 2021) <http://www.techopedia.com/definition/27960/web-10> accessed 22 May 2022.
[47] Jon Garon, 'Legal Implications of a Ubiquitous Metaverse and a Web3 Future' (2022), 11 <http://dx.doi.org/10.2139/ssrn.4002551> accessed July 14 2022.
[48] Burke (n 42) 8.

to by experts such as Chris Dixon as the 'read, write, own' web.[49] This is in reference to the growing interest in Web 3.0 companies that value data sovereignty and use decentralized technologies, such as blockchain and NFTs. While these are promising developments that aim to solve many of the issues experienced in Web 2.0, it should also be noted that the global and decentralised nature of Web 3.0 poses a significant governance challenge for the future.[50]

The most significant aspect of the evolutionary process of the internet is the legislative framework that has slowly emerged to regulate Web 2.0 on account of the ethical quandaries that have transpired over the past two decades. Data breaches and other privacy violations caused by bad actors and the clandestine data collection practices of Web 2.0 companies have been the focus of internet regulation to date. The European Union has been a frontrunner in this respect, adopting the GDPR in 2016 which improved global standards of data protection.[51] Two years later, the CCPA was adopted in California which set out similar data subject rights as the GDPR.[52] In parallel to this, an active digital rights community has succeeded in gaining recognition for the extension of human rights to the internet. Such rights typically relate to the right to privacy and freedom of expression online.[53] However, these developments are reactionary in nature because they respond only to specific data protection and security threats and attempt to retrofit solutions to digital problems after the technologies have already been on the market for some years. This becomes worrisome when one considers that the metaverse will not only pose the same issues that we struggled to solve in Web 2.0, but it will also introduce new ethical challenges that the existing regulatory framework is ill-equipped to deal with. Interestingly, a wave of forthcoming EU legislation, particularly the proposed new Data Governance Act, focuses on placing control back in the hands of the individual, in line with Web 3.0 the trends that favour data sovereignty and ownership.[54] This will challenge the attempts of Web 2.0 companies, such as Meta, to maintain their monopolies over user-generated data in Web 3.0.

---

[49] Chris Dixon [@cdixon], 'Web1: Read Web2: Read, Write Web3: Read, Write, Own' *Twitter* (8 February 2022) <https://twitter.com/cdixon/status/1490866307599794180> accessed 22 May 2022.
[50] Dean Takahashi, 'The Ethics of the Metaverse' *VentureBeat* (27 January 2022) <https://venturebeat.com/2022/01/26/the-ethics-of-the-metaverse-2/> accessed 22 May 2022.
[51] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/32.
[52] Title 1.81.5. California Consumer Privacy Act of 2018 [1798.100 1798.199.100] ch 55, sec 3.
[53] Rosamund Hutt, 'What Are Your Digital Rights?' World Economic Forum (13 November 2015) <https://www.weforum.org/agenda/2015/11/what-are-your-digital-rights-explainer/> accessed 22 May 2022.
[54] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) [2020] COM/2020/767 final.

In short, Web 3.0 technologies will pose new threats to human rights protection that were unforeseen by regulators. Therefore, existing legislation will be rendered ineffectual unless the necessary changes and updates are made before the coalescence of the metaverse. However, regulators do not necessarily need to reinvent the wheel when it comes to metaverse governance. This paper argues that the majority of legislative loopholes that the metaverse exposes can be addressed by making updates to existing legislation and deriving lessons learned from previous attempts to regulate the internet, social media, and video games. This will also help to prevent confusion and fragmentation of the regulatory framework as Web 3.0 emerges.

Zuckerberg's Vision for the Metaverse

Within the context of this historical background, the focus of this paper is on the Web 3.0 technologies Meta is developing for the metaverse and their potential human rights implications. This first warrants a discussion on the ongoing projects at Facebook Reality Labs. Zuckerberg introduced a number of these projects at the company's 2021 Connect Conference, along with his broader vision for the future metaverse. He envisions it to be a space where users will spend a considerable amount of their time, whether it be gaming, shopping, working, learning, or socialising.[55] His technologies focus on achieving a seamless interaction with this new digital world that will be as easily accessible as the current internet.

Project Nazare

Project Nazare is the codename for a pair of augmented reality glasses that Meta had initially planned to release commercially before 2024. However, as of June 2022, reports suggest that the first iteration of these glasses will be retained for developers, with subsequent versions becoming available to consumers further down the line.[56] Early versions of the device will contain eye-tracking sensors, a front-facing camera, and stereo audio contained within the frame of a pair of normal-sized glasses that can project interactive holographic images in front of the wearer.[57] Last year, Facebook collaborated with Ray-Bans to release their first pair of smart glasses called Ray-Ban-Stories. Retailing at $299, the smart glasses contain speakers on

[55] Meta (n 7).
[56] Sylvia Varnham O'Regan, 'Meta Scales Back AR Glasses Plan Amid Reality Labs Shakeup' *The Information* (9 June 2022) <https://www.theinformation.com/articles/meta-scales-back-ar-glasses-plan-amid-reality-labs-shakeup> accessed 22 June 2022.
[57] Alex Heath, 'Mark Zuckerberg's Augmented Reality' *The Verge* (13 April 2022) <https://www.theverge.com/23022611/meta-facebook-nazare-ar-glasses-roadmap-2024> accessed 19 April 2022.

either side of the frame, a touchpad, and two front-facing cameras that can record photos and videos at the push of a button, or by saying 'Hey Facebook, take a video.' The glasses sync to a mobile app in order to save the recorded footage.[58] Project Nazare will build on this technology to offer a more interactive AR experience.

Wrist-worn device

Facebook Reality Labs are also creating a wearable wrist-based device that will work in conjunction with its AR glasses. The device will use neural interfaces in the wrist to detect hand movements and allow the user to control their environment in AR.[59] The novel science of electromyography will be employed to translate these hand movements into commands. Examples of such commands include moving virtual objects and high-speed typing, as demonstrated at the 2021 Connect Conference.[60] The aim of creating this kind of wearable is to allow users to interact more intuitively with the metaverse. According to Meta's researchers, the contemporary use of mobile phones is rather unnatural because they draw the user's attention down to a small, handheld device.[61] By contrast, non-invasive brain-computer interface devices such as this would make it easier for individuals to navigate mixed reality settings.

Haptic glove

Haptic technology will allow users to experience the sense of touch in the metaverse. While Meta's Oculus Quest has already developed hand tracking controllers that create a digital version of one's hands in VR, Facebook Reality Labs are creating a lightweight haptic glove device that will increase one's dexterity and fidelity in the metaverse. The gloves will simulate the sensations of pressure, texture, and vibration when interacting with virtual objects.[62] In November of 2021, Meta also announced the development of ReSkin, a thin membrane-like robot skin, that was created by AI researchers in collaboration with Carnegie Mellon

[58] Alex Heath, 'Facebook Debuts Ray-Ban Stories, Smart Glasses That Record Video' *The Verge* (9 September 2021) <https://www.theverge.com/2021/9/9/22662809/facebook-ray-ban-stories-camera-smart-glasses-hands-on> accessed 22 May 2022.
[59] Meta (n 7) 1:07:10.
[60] ibid.
[61] 'Inside Facebook Reality Labs: Wrist-Based Interaction for the next Computing Platform' *Tech at Meta* (18 March 2021) <https://tech.fb.com/ar-vr/2021/03/inside-facebook-reality-labs-wrist-based-interaction-for-the-next-computing-platform/> accessed 22 May 2022.
[62] 'Inside Reality Labs Research: Meet the Team That's Working to Bring Touch to the Digital World' *Tech at Meta* (16 November 2021) <https://tech.fb.com/ar-vr/2021/11/inside-reality-labs-meet-the-team-thats-bringing-touch-to-the-digital-world/> accessed 22 May 2022.

University.[63] This technology will likely be incorporated into its haptic glove to bring an even greater sense of reality to the metaverse.

Project Cambria

Meta acquired the market-leading company Oculus VR in 2014.[64] Now rebranded as Meta Quest, the acquisition has proven successful by producing a top-of-the-line VR headset that can be used on Meta platforms such as Horizon Worlds.[65] Meta's newest headset, dubbed Project Cambria, is set to build on this success by introducing mixed reality interactions. The wireless device will provide improved optics, sensors, and high-definition full-colour passthrough that will render interactions in the metaverse more natural for the user. For example, it will allow natural eye contact to be made between avatars and will replicate facial expressions in real time. The headset will also be designed to realistically represent the physical world to allow users to work and exercise in mixed reality settings.[66] Additionally, project Cambria will work in conjunction with Meta's new AR Presence Platform which was unveiled at the 2021 Connect Conference.[67]

Codec Avatars

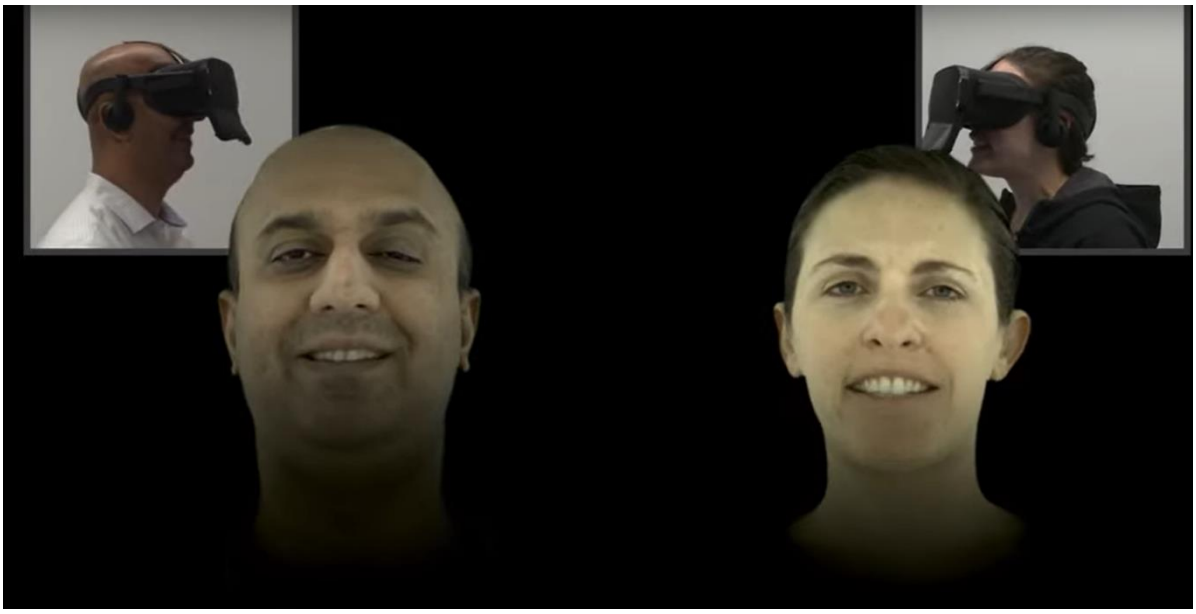
One much-lauded technology is the development of Codec Avatars by Facebook Reality Labs. These hyper-realistic avatars are central to Meta's aim of achieving a 'social presence' in its vision for the future metaverse. The Director of Research at Facebook Reality Labs, Yaser Sheik, has referred to 'social presence' in the following context: "you have to love your avatar and your mother has to love your avatar before the two of you feel comfortable interacting like you would in real life."[68] Considering this, Codec Avatars are described as 'learned, photorealistic face models that accurately represent the geometry and texture of a person in 3D (i.e., for virtual reality), and are almost indistinguishable from video.'[69] It should be noted that while the technology currently only portrays the face and head of the user, Meta's researchers

---

[63] Raunaq Bhirangi and others, 'ReSkin: versatile, replaceable, lasting tactile skins' (2021) 5th Conference on Robot Learning <https://reskin.dev/?fbclid=IwAR2G39gcfVuDpy1uru6qNds47N5QwWJtztSkgZUlrXJXSDJpYxKgyu2nvF0> accessed 22 May 2022.
[64] Egliston, and Carter (n 18).
[65] ibid.
[66] Meta Quest, 'Project Cambria Preview - Mixed Reality with Presence Platform' (12 May 2022) <https://www.youtube.com/watch?v=tgJ7m0Phd64> accessed 22 May 2022.
[67] ibid.
[68] 'Facebook is Building the Future of Connection with Lifelike Avatars' *Tech at Meta* (13 March 2019) <https://tech.fb.com/ar-vr/2019/03/codec-avatars-facebook-reality-labs/> accessed 23 May 2022.
[69] 'Audio- and Gaze-Driven Facial Animation of Codec Avatars' *Meta Research* (17 December 2021) <https://research.facebook.com/videos/audio-and-gaze-driven-facial-animation-of-codec-avatars/> accessed 19 April 2022.

have expressed their intentions to eventually create detailed full-body replicas of our physical likeness.[70] As illustrated in Figure 1, the Codec Avatar technology perfectly replicates the appearance of two Meta researchers wearing Oculus VR headsets in real-time.

Figure 1. Codec Avatars



Source: Meta Quest, 'Codec Avatars' (25 Sept 2019) <https://www.youtube.com/watch?v=Rqj956KgvRU> accessed 20 April 2022.

These avatars are powered by cutting-edge 3D capture technology that tracks motion and facial expressions to deliver high-fidelity virtual avatars. Advancements in machine learning and AI will allow individuals to interact through their Codec Avatars in real-time.[71] Currently, the process of creating a Codec Avatar is very cumbersome, but researchers aim to simplify this process to allow users to create their own avatars from just a few images of themselves.[72] This process requires the collection of accurate data on the subtlest facial expressions, such as the darting motion of an eye, the puffing of one's cheeks, the scrunching of a nose, and the furrowing of an eyebrow, as well as smaller physical details such as a person's teeth and hair.[73] This precise attention to detail will help to achieve a sense of realism and avoid the unwanted 'uncanny valley' effect in response to Codec Avatars. In conversation with scientist Michael Abrash at the 2021 Connect conference, Zuckerberg also demonstrated the ability to update the

[70] Meta Quest, 'Full-Body Codec Avatars' (25 September 2019) <https://www.youtube.com/watch?v=_ZkG4iB_exU> accessed 23 May 2022.
[71] 'Facebook Is Building the Future of Connection with Lifelike Avatars' (n 68).
[72] ibid.
[73] Meta Quest, 'Codec Avatars' (25 September 2019) <https://www.youtube.com/watch?v=Rqj956KgvRU> accessed 2 April 2022.

appearance of a 3D avatar to match changes in one's own physical appearance.[74] The example he gives is of a male user who decides to shave his beard and how this can be reflected by the technology with incredible accuracy (see Figure 2). A truly interoperable metaverse will allow these changes to be reflected across all platforms, regardless of whether Meta owns the platform or not.

Figure 2. Changes to the Appearance of a 3D Avatar

Source: Meta, 'The Metaverse and How We'll Build It Together -- Connect 2021' (28 October 2021) <https://www.youtube.com/watch?v=Uvufun6xer8> accessed 27 March 2022.

Considering the hyper-realistic nature of these Codec Avatars and their ability to change in response to the user's real-life appearance, a nuanced discussion about the term 'digital twin' is necessary here. Digital twins are virtual representations of physical objects. They are created by feeding a simulator with vast amounts of both historic and real-time data to generate an exact digital replica of an object. Typically, they are employed in the engineering sector to test a prototype for flaws or unforeseen risks, which helps the industry by cutting costs and protecting the physical object.[75] Given that the metaverse will essentially become a digital replica of the physical world, digital twins will make up the architecture of this virtual space and will be used to populate it with complex simulations of buildings and objects.[76] Similarly, Codec Avatars are exact replicas of the physical person that feed off live data obtained from the user that will allow the model to be constantly updated. The type of data that is collected

[74] Meta (n 7) 1:03:10.
[75] Saeed Banaeian Far and Azadeh Imani Rad, 'Applying Digital Twins in Metaverse: User Interface, Security and Privacy Challenges' (2022) 2(1) Journal of Metaverse 8, 8.
[76] Theo Priestley, 'Digital Twins, IOT and the Metaverse' *Medium* (5 August 2021) <https://medium.com/@theo/digital-twins-iot-and-the-metaverse-b4efbfc01112> accessed 22 April 2022.

throughout this process goes much further than the static digital or shadow profiles that Meta currently keeps about its user base.[77] Moreover, these avatars pose similar legal challenges to those associated with digital twins, such as ambiguities surrounding intellectual property rights, data protection, and liability if something goes wrong. Hence, this paper argues that Codec Avatars should also be considered digital twins in the metaverse.

Meta is developing ground-breaking technologies at Facebook Reality Labs to bring its vision for the metaverse to life. These new technologies could potentially bring great benefits to humanity by facilitating the right to education through immersive learning and improved access to information,[78] promoting skills development and employee training using VR simulations,[79] protecting the right to the highest attainable standard of health by allowing for remote AR/VR interactions with patients to control infection rates during health emergencies such as the COVID-19 pandemic,[80] and improving the quality of life of people living with disabilities through immersive experiences.[81] However, they also pose many legal and ethical questions that must be addressed to prevent mass-scale violations of human rights. How will Meta ensure the biometric data it collects remains secure? What will consent for the processing of sensitive data look like in the metaverse? Is it legal for Meta to process unconscious facial expressions that reveal intimate details about the user without their consent and for the purposes of targeted advertising? Should users have legal ownership over their avatars or at least the data used to build them? How will women be protected from the pervasive phenomenon of virtual sexual harassment? What are the consequences of children seeing and experiencing inappropriate behaviour in the metaverse? Who is accountable for avatars that perpetuate violence against others, and can they be punished for these crimes? These issues are summarised in Table 1 below and the following chapters will aim to address them in more detail.

[77] Russell Brandom, 'Even If You're Not Signed up, Facebook Has a Shadow Profile for You' *The Verge* (11 April 2018) <https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy> accessed 23 April 2022.
[78] Guido Makransky and Richard E. Mayer, 'Benefits of Taking a Virtual Field Trip in Immersive Virtual Reality: Evidence for the Immersion Principle in Multimedia Learning' (2022) Educ Psychol Rev <https://doi.org/10.1007/s10648-022-09675-4> accessed 25 June 2022.
[79] Mark Purdy, 'How the Metaverse Could Change Work' Harvard Business Review (5 April 2022) <https://hbr.org/2022/04/how-the-metaverse-could-change-work> accessed 25 June 2022.
[80] Jane Thomason, 'MetaHealth - How will the Metaverse Change Health Care?' (2021) 1(1) Journal of Metaverse 13 <https://dergipark.org.tr/en/download/article-file/2167692> accessed June 25, 2022.
[81] Rian Dutra da Cunha, Francila Weidt Neiva and Rodrigo Luis de Souza da Silva, 'Virtual Reality as a Support Tool for the Treatment of People with Intellectual and Multiple Disabilities: A Systematic Literature Review' (2018) 25(1) Revista de Informática Teórica e Aplicada 67.

Table 1. Taxonomy of the human rights implications of Zuckerberg's metaverse

Issue	Major Concerns	Human Right(s) Affected	Legal Response	Potential Solutions
Intensive biometric data collection	Data breaches; avatar impersonation	The right to privacy	Public law (biometric law, data protection law)	Data minimisation; security by design; liveness detection
Obtaining consent for data processing	Users unaware of the purposes of data collection	The right to privacy	Public law (biometric law, data protection law)	Clarification of valid consent in the metaverse
Biometric psychography	Use of subconscious reactions to individualise ads without consent; surveillance capitalism	The right to privacy; freedom of thought; freedom from discrimination	Public law (biometric law, data protection law, international human rights law)	Update the definition of biometric data; reassess the UNGPs; the right to mental privacy
Avatar ownership	Adverse impacts on the mental health and human dignity of users if their avatar is harmed	The right to health; freedom from degrading treatment	Private law (property law)	Data ownership, legal personality for avatars
Sexual harassment	Women and children experience sexual abuse in immersive reality	Freedom from discrimination; freedom from degrading treatment	Public law (criminal law, international human rights law); Private law (civil law);	Legal recognition of virtual sexual harassment (and assault/rape in the future); change in societal attitudes; corporate responsibility to protect

Interim Conclusions

Dr Thomas Furness is an American inventor who is often referred to as the grandfather of VR. He has likened immersive technologies to discoveries such as atom-splitting or fire, a development that 'can be used for helping mankind, lifting mankind, or it can be used for destroying mankind.'[82] This highlights the crossroads at which we stand when it comes to the metaverse. The technologies under development at Facebook Reality Labs have the power to transform the way we connect with others and conduct business. However, they will also collect an unprecedented amount of sensitive user data and will introduce new means of interacting with others in digital environments. This poses several unforeseen legal issues and a multitude of new threats to safeguarding human rights. It is, therefore, critical to identify the

[82] Heller (n 17).

specific human rights that are at stake and inform regulators of how the legal framework can be updated accordingly.

Chapter 2: Transgressions of the Right to Privacy and Data Protection

This chapter addresses some of the potential ways in which Meta's new technologies may interfere with the right to privacy. First, it will provide a brief overview of the international legal framework as it pertains to the right to privacy and the right to data protection, with specific reference to EU law. It then identifies three core legal issues associated with the right to privacy in Zuckerberg's metaverse: (1) the security of biometric data processed for the purpose of building Codec Avatars; (2) ambiguities surrounding what constitutes valid consent for such data processing; and (3) the loophole in existing legislation that permits biometric psychography. If these legislative gaps are not closed it will have broader societal impacts by perpetuating an economy of surveillance capitalism that does not respect the right to privacy. This leads to the final part of this chapter which is concerned with freedom of thought in the metaverse and begs the question of whether the right to privacy should extend to mental privacy in the metaverse age.

The Right to Privacy in International Law

Contemporary understandings of the right to privacy emanate from a seminal 1890 article written by two American lawyers, Samuel Warren and Louis Brandeis. In the article, Warren and Brandeis argue that on account of the press overstepping personal boundaries in the pursuit of reporting gossip about celebrities, the natural evolution of the law is to safeguard one's 'right to be let alone.'[83] This set the legal precedent for American legislation regarding privacy, which subsequently influenced international human rights law. The right to privacy is a fundamental human right enshrined in article 17 of the International Covenant on Civil and Political Rights (ICCPR)[84] and Article 12 of the Universal Declaration of Human Rights[85], along with several regional human rights doctrines. Central to this right is the tenet of human dignity; respect for the privacy of one's family life, home, and correspondence protects the autonomy and personal identity of the individual and complements the enjoyment of other rights.[86]

[83] Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4(5) *Harvard Law Review* <https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html> accessed 26 April 2022.
[84] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) art 17.
[85] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR) art 12.
[86] UNCHR 'The Right to Privacy in the Digital Age - Report of the United Nations High Commissioner for Human Rights' (30 June 2014) UN Doc A/HRC/27/37, 5 para. 14.

Akin to Warren and Brandeis' assertion that an evolution of the law was needed to reign in the excesses of the press, innovative technologies of the 21st century pose unforeseen threats to the right to privacy. This has coincided with the exponential growth of technology companies that now wield considerable influence over the personal lives of their users. Meta, for example, has accumulated more personal data on its users than any other platform, which has contributed greatly to its success.[87] For this reason, the soft law of the United Nations imposes a due diligence requirement on states to enact appropriate legislation to uphold the right to privacy in the face of these new challenges. For example, Pilar I of the Guiding Principles on Business and Human Rights obliges states to take steps to mitigate potential human rights abuses by businesses through 'effective policies, legislation, regulations, and adjudication.'[88]

Considering this, data protection has emerged as the primary legal mechanism through which the right to privacy is protected in the digital environment. This was codified into international law as early as 1981 when the Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The convention was revised in 2018 and now forms the foundation of data protection law in 40 European countries.[89] It is also open to accession to non-Member States to reflect the transboundary nature of technology and its impacts. In addition, the EU Data Protection Directive of 1995 was an influential piece of legislation that shaped global norms regarding the processing and movement of personal data.[90] However, arguably the most influential European data protection legislation is the GDPR which was adopted by the EU in 2016 and entered into force in 2018.[91] This document led to a wave of similar bills being passed in other parts of the world and defined the EU as a bulwark for the right to privacy in the digital age and for protecting human rights online.

On account of these developments, this chapter focuses predominantly on the interaction between Meta's metaverse technologies and EU data protection legislation and the case-law of the European Court of Justice. Moreover, this chapter will treat the right to data protection as a component of the right to privacy as it pertains to data collection and processing in the

[87] Surfshark, 'Apps That Track You and Their Alternatives' <https://surfshark.com/apps-that-track-you> accessed 25 June 2022.
[88] OHCHR, 'Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework' (16 June 2011) UN Doc HR/PUB/11/104, 3.
[89] Council of Europe, 128th session of the Committee of Ministers 'Convention 108+: Convention for the protection of individuals with regards to the processing of personal data' (18 May 2018).
[90] Clément Perarnaud, 'Privacy and Data Protection' *DW Observatory* <https://dig.watch/topics/privacy-and-data-protection> accessed 27 April 2022.
[91] GDPR (n 51).

metaverse. However, I do concede that once the novel idea of the metaverse has fully coalesced, it may be deemed to fall outside the scope of current data protection legislation such as the GDPR. Therefore, I refer to certain will provisions of the Regulation throughout this chapter as a means of highlighting where Meta's technologies infringe upon international data protection standards and norms that were formalised by the GDPR.

Privacy Issues Associated with the Collection of Biometric Data for Codec Avatars

The hardware devices that Meta is developing for the metaverse will give the company unprecedented access to users' private lives. For example, in line with Project Aria, its AR glasses will be designed to collect the necessary data to build a live 3D virtual map of the user's surroundings.[92] Not only will this entail the use of GPS location tracking, but it also suggests that the glasses will be constantly recording what the wearer sees, hears, and does, even in their own homes.[93] These privacy concerns are exacerbated by the inconspicuous recording function that was included in the recently launched Ray-Ban Stories glasses. This feature allows wearers to easily record other individuals without their knowledge and perhaps identify them if subsequent versions of the glasses are fitted with facial recognition technology, an idea that Facebook's researchers are currently toying with.[94] This raises concerns about the amount and the type of data Meta intends to collect in order to achieve its metaverse ambitions.

In addition to this, Meta's Codec Avatars will demand a great deal of users' personal data, including information about their biological characteristics. This may include but is not limited to gait, voice recognition, the mapping of facial patterns, and iris recognition. These biological and physiological identifiers are known as biometrics or biometric data.[95] The harvesting of such data comes with a number of risks, most notably security breaches and the issue of obtaining valid consent from data subjects. Hence, biometrics constitute a special category of data that is afforded additional protection by national and international laws. For example, article 4 (14) of the GDPR defines biometric data as 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as

[92] Meta, 'Introducing Project Aria' <https://about.facebook.com/realitylabs/projectaria/> accessed 9 June 2022.
[93] Katitza Rodriguez and Kurt Opsahl, 'Augmented Reality Must Have Augmented Privacy' *Electronic Frontier Foundation* (16 October 2020) <https://www.eff.org/deeplinks/2020/10/augmented-reality-must-have-augmented-privacy> accessed 25 June 2022.
[94] Ryan Mac, 'Facebook Is Considering Facial Recognition For Its Upcoming Smart Glasses' *BuzzFeed News* (25 February 2021) <https://www.buzzfeednews.com/article/ryanmac/facebook-considers-facial-recognition-smart-glasses> accessed 9 June 2022.
[95] Heller (n 17) 15.

facial images or dactyloscopic data.'[96] Article 9 of the Regulation prohibits the processing of biometric data unless the explicit consent of the individual is obtained or the processing of such data is strictly necessary to protect the interests of the data subject or the rights of the controller.[97] Any violation of these provisions is typically met with a large fine, as demonstrated by the EUR 20 million fine recently handed down by the Italian data protection agency to the controversial tech company Clearview AI for using facial recognition to process data subjects' biometric data without their consent.[98] Nevertheless, the possession of biometric data is particularly advantageous to ad tech companies like Meta as they reveal surprisingly accurate insights into the individual's personality and future behaviour. This presents a paradox for the future as big tech companies balance their legal obligations with commercial interests in the metaverse.

Security Issues

The deeply personal nature of biometric data can easily lead to a violation of the right to data protection in the event of a security breach. Traditional data breaches may leak sensitive information such as the user's phone number, email address, or passwords, the consequences of which are temporary as the user often has the chance to change this information to prevent further interference with their privacy rights. By contrast, the repercussions of a breach of biometric data are much greater as one cannot change their fingerprint or facial pattern as easily as they would a password.[99] Hence, the repercussions of a biometric data breach can last a lifetime for affected data subjects.

To make matters worse, Facebook has a poor track record when it comes to the security of users' data, appearing twice on a list of the biggest data breaches in history.[100] As a consequence of this, 87% of respondents to a 2022 survey conducted by NordVPN expressed concerns that their privacy could be affected by a Meta-led metaverse.[101] Moreover, while article 33 of the GDPR calls for data controllers to notify users within 72 hours of a data

[96] GDPR (n 51) art. 4 para. 14.
[97] Ibid (n 51) art. 9.
[98] *Ordinanza ingiunzione nei confronti di Clearview AI* [2022] Guarante per la Protezione dei Dati Personali 9751362.
[99] Avi Bar-Zeev, 'For XR, the Eyes Are the Prize' *Medium* (17 November 2020) <https://avibarzeev.medium.com/for-xr-the-eyes-are-the-prize-25d43a533f2a> accessed 30 April 2022.
[100] Abi Tyas Tunggal, 'The 63 Biggest Data Breaches (Updated for February 2022)' *UpGuard* (26 June 2022) <https://www.upguard.com/blog/biggest-data-breaches> accessed 30 April 2022.
[101] Karolis Bareckas, 'Would You Join the Metaverse?' *NordVPN* (25 January 2022) <https://nordvpn.com/blog/metaverse-survey/> accessed 28 May 2022.

breach,[102] what mitigating effect does this have when the consequences are lasting and individuals cannot do anything to protect themselves? If the company decides to store the biometric data of millions, or even billions, of users on a central database it will become a prime target for bad actors. In a recent speech at the 2022 IAPP Summit, Apple CEO Tim Cook stated that 'centralized, readable data is vulnerable data.'[103] For these reasons, Meta should take steps to minimize the amount of biometric data it collects and consider how the necessary data can be anonymized and stored securely to mitigate the effects of a data breach. It should also apply the principle of security by design to all metaverse-related technologies and must be held to account if the necessary safeguards are not put in place to protect the privacy of its users.

Security of information will be key to encouraging the adoption of metaverse technologies. However, this will also prove to be one of the most difficult aspects of creating the metaverse, since every 'state of the art' security system ultimately has the potential to be hacked.[104] Experts have also highlighted the difficulties associated with detecting cyber-attacks in the metaverse due to the vast amount of infrastructure that will be built by different actors with varying levels of security in mind.[105] Endless social engineering opportunities will exist for fraudsters attempting to extract financial information and other sensitive data from users. For example, if a bad actor manages to hack the identity of a friend, family member, or co-worker, they may be able to convince users to give up sensitive information by posing as their Codec Avatar.[106] For this reason, many companies are currently working on solutions to securing digital identities in the metaverse in a way that is seamless and non-disruptive to the immersive experience. This will likely entail matching a person's selfie with their ID, coupled with liveness detection to verify that the person is there and not a fraudster posing with a photo or a mask.[107] However, these security issues also raise the question of whether anonymity will be

[102] GDPR (n 51) art. 33.
[103] International Association of Privacy Professionals, 'LIVE IAPP Summit 2022 General Session with Tim Cook, Zahra Mosawi, Didier Reynders and Trevor Hughes' (12 April 2022) 20:10 <https://youtu.be/Dq0fcmmzfog?t=11> accessed 28 May 2022.
[104] Rob Davies, '"Conditioning an Entire Society": The Rise of Biometric Data Technology' *The Guardian* (26 October 2021) <https://www.theguardian.com/technology/2021/oct/26/conditioning-an-entire-society-the-rise-of-biometric-data-technology> accessed 26 June 2022.
[105] Kyle Alspach, 'Why the Fate of the Metaverse Could Hang on Its Security' *VentureBeat* (26 January 2022) <https://venturebeat.com/2022/01/26/why-the-fate-of-the-metaverse-could-hang-on-its-security/> accessed 28 May 2022.
[106] ibid.
[107] Alexey Khitrov, 'What Will It Take to Stop Fraud in the Metaverse?' *Information Age* (29 March 2022) <https://www.information-age.com/what-will-it-take-to-stop-fraud-in-metaverse-123499073/> accessed 28 May 2022.

an option for users in the metaverse considering the potential for bad actors to get away with harmful behaviour.

Obtaining consent

As noted above, the GDPR requires the explicit consent of the data subject to be obtained prior to his or her biometric data being processed by the data controller. Article 4(11) of the Regulation defines consent as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.'[108] However, this definition allows for a certain degree of interpretation on behalf of data controllers as to how consent may be obtained. Hence, one must look to the case law of the European Court of Justice for clearer guidelines on the rules around biometric data processing.

A 2019 ruling by the Court in the case of Plantet49 was the first to deal exclusively with the issue of consent since the Regulation entered into force in 2018. The case concerned a German online gaming company that used a pre-ticked box as a form of obtaining consent before processing users' personal data.[109] The Court's judgment in the case clarified that explicit, or active, consent is the only valid form of consent regardless of the type of data being processed. Therefore, explicit consent can be understood as an affirmative action that must be performed on behalf of the data subject, e.g., the ticking of a box.[110] The EDPB published guidelines on consent under the GDPR in May 2020 which complement the legal precedent set by the European Court in this case. The guidelines give examples of how explicit consent can legally be obtained in the digital context, such as 'filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature.'[111]

However, it is unclear how the consent mechanisms designed for web 2.0 data processing will translate to the metaverse. If Zuckerberg wishes to create a seamless blend between the real and the virtual worlds, it is likely that users regularly having to fill out an electronic consent

[108] GDPR (n 51) art 4 para 11.
[109] Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband v. Planet49 GmbH* [2019] ECR 801.
[110] Court of Justice of the European Union Press Release No. 125/19, 'Storing cookies requires internet users' active consent' (1 October 2019) <https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-10/cp190125en.pdf> accessed 28 May 2022.
[111] European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (4 May 2020) 21, para. 94 <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 28 May 2022.

form to agree to each purpose for which their personal data is processed does not factor into this vision. Another possibility is that the tech company will attempt to circumvent its obligations under the GDPR. Meta's data collection practices have already come under fire from Austrian data privacy activist Max Schrems as demonstrated by the Schrems v Facebook Ireland (2021) case which is currently pending a decision by the European Court of Justice.[112] Schrems has accused Meta of bypassing its GDPR obligations by treating consent as a civil law contract that deprives users of the many rights bestowed upon them by the Regulation while empowering the tech giant to leverage user data against them in the form of targeted advertisements.[113] This will likely be a landmark case, the outcome of which will define the parameters of obtaining explicit consent in the metaverse.

Biometric Psychography in the Metaverse as a Gateway to Surveillance Capitalism

A business model 'predicated on human rights abuse'?

On January 18, 2022, the Financial Times unveiled Meta's plans to use biometric data to target personalised advertisements towards users in the metaverse. This revelation is supported by hundreds of patent applications filed by the technology company to the United States Patent and Trademark Office, the federal agency responsible for granting such applications.[114] This demonstrates an intention by Meta to replicate its lucrative commerce-led, ads-based business model in the metaverse, using even more sensitive and personal information about its customers. This is one of the key reasons why experts believe that Meta will not support an open, decentralised metaverse. An ads-based economy controlled by one company has all the manifestations of a closed, walled garden platform. Furthermore, at the 2021 Connect conference, Zuckerberg stated that Meta would sell its new devices at cost or lower to boost innovation and encourage adoption at the preliminary stages of development.[115] In turn, the company will generate revenue from targeted advertisements, as confirmed by Nick Clegg, Meta's President of Global Affairs.[116] This implies that users will have to give up a certain level of data privacy as a trade-off to access Meta's envisioned metaverse.

[112] Case C - 446/21 *Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 20 July 2021 — Maximilian Schrems v Facebook Ireland Ltd* [2021] OJ C 422/08.
[113] Reuters, 'Austrian Activist Schrems' Facebook Complaint Referred to EU Court' (20 July 2021) <https://www.reuters.com/technology/austrian-activist-schrems-facebook-complaint-referred-eu-court-2021-07-20/> accessed 2 May 2022.
[114] Murphy (n 1).
[115] Meta (n 7) 35:20.
[116] Murphy (n 1).

Article 6 (1) (e) of the GDPR requires consent to be obtained for each specific purpose for which personal data is used.[117] Therefore, collecting biometric data for the purpose of creating a Codec Avatar and then using this data to inform marketing decisions without the consent of the data subject would violate the provisions of the Regulation. The GDPR could benefit from a more explicit prohibition of such practices, such as that contained in as Illinois' 2008 Biometric Information Privacy Act (BIPA). The BIPA is the first law of its kind in the US to aim specifically at regulating biometric data.[118] Section 15 (c) of the Act prohibits private entities from profiting from people's biometric data.[119] In recent times, Clearview AI has been forced to pull out of offering its infamous data scraping services to law enforcement in the state for fear of being found to be in violation of the law.[120] Meta would likely take the same approach in this case since the BIPA only protects residents of Illinois and it is relatively easy for such a large company with a presence in almost every country to bypass.

However, neither the GDPR nor the BIPA prevent businesses from profiting off inferences made from users' biometric data, such as their likes, dislikes, motivations, or interests.[121] This constitutes a major loophole in existing data protection legislation that lawmakers could not foresee even a few years ago. To achieve realistic social presence in the metaverse, hardware such as Project Cambria and Project Nazare will process a huge amount of sensitive, personal information about the user, by tracking their eye movements, pupil dilation, heart rate, blood pressure, and potentially even brain waves. For example, VR headsets track eye movements to apply foveated rendering which blurs the user's peripheral vision in order to enhance the visual realism of the experience and reduce simulation sickness.[122] In addition, AR glasses use eye-tracking sensors to determine what object the user wishes to interact with.[123] However, these eye-tracking technologies can also be used to infer deeply personal insights about the user's private life. The problem with existing legislation is that it reflects the outdated concept that a person must be identified from their biometric data in order for their privacy to be intruded upon. Meanwhile, the inferences that can be made from biometric data collected by forthcoming metaverse technologies are not linked to one's identity and can thus be obtained

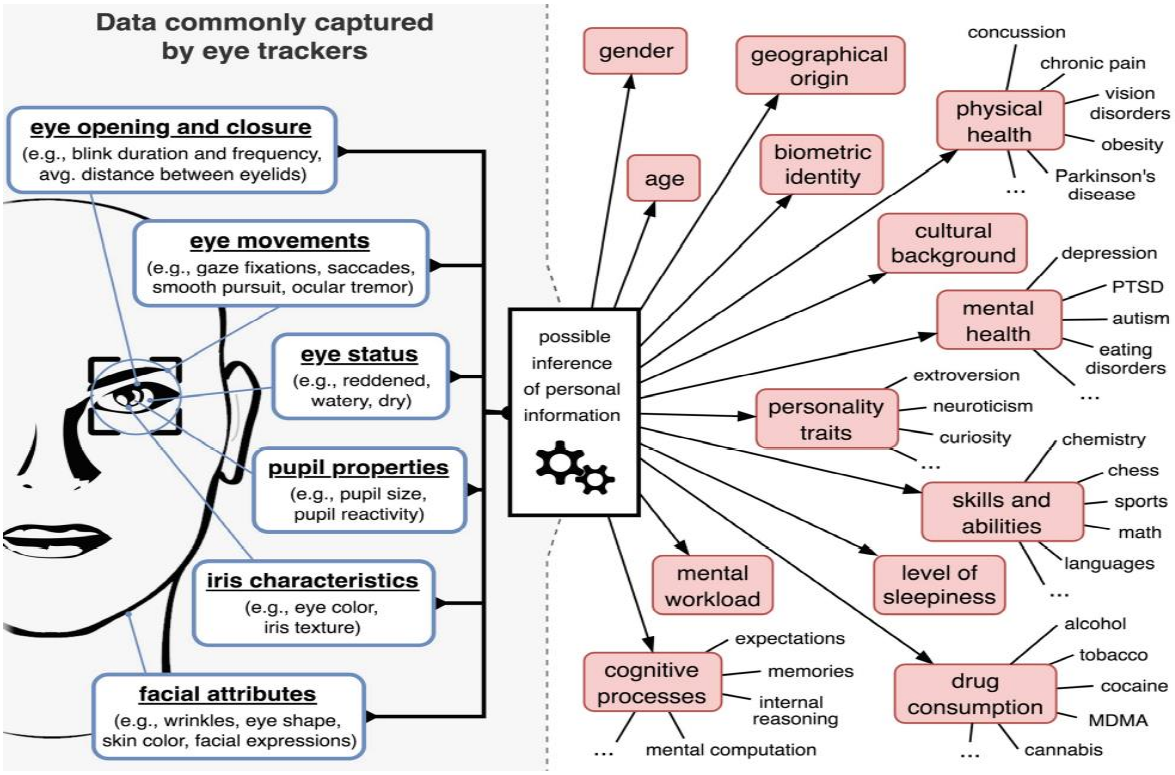
[117] GDPR (n 51) art 6(1) para e.
[118] Woodrow Hartzog, 'BIPA: The Most Important Biometric Privacy Law in the US?' in Amba Kak (ed) *Regulating Biometrics: Global Approaches and Urgent Questions* (AI Now Institute 2020) 96.
[119] Ibid, 97.
[120] Ibid, 110.
[121] Heller (n 17) 14.
[122] ibid, 3.
[123] Meta (n 7) 1:01:10.

without the informed consent of the individual.[124] This presents a major threat to the right to privacy if Meta intends to use this information to tailor advertisements towards us in the metaverse.

Multiple studies have shown that physiological behaviours such as eye movements, hand gestures, and facial expressions are often involuntary and conducted instinctively by the individual based on his or her surroundings. For example, the eye uses 'smooth pursuit' movements to follow moving objects, while saccades are darting motions that are used to locate objects of visual interest. The eye interchanges between both types of movement without the individual noticing or actively making the changes.[125] Given up subconsciously, these data reveal deeply personal insights about an individual. A 2020 study revealed that eye-tracking data can divulge details not only about one's age, ethnicity, gender, and personal interests, but also intimate knowledge about their sexual preferences, mental health, and drug consumption habits (see Figure 3 below).[126]

[124] Heller (n 17) 14.
[125] Avi Bar-Zeev (n 99).
[126] Jacob Leon Kröger, Otto Hans-Martin Lutz and Florian Müller, 'What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking' in Michael Friedewald, Melek Önen, Eva Lievens, Stephan Krenn and Samuel Fricker (eds), *Privacy and Identity Management. Data for Better Living: AI and Privacy* (Springer 2020) <https://link.springer.com/chapter/10.1007/978-3-030-42504-3_15> accessed 26 June 2022.

Figure 3. Inferences Made from Eye-Tracking Data

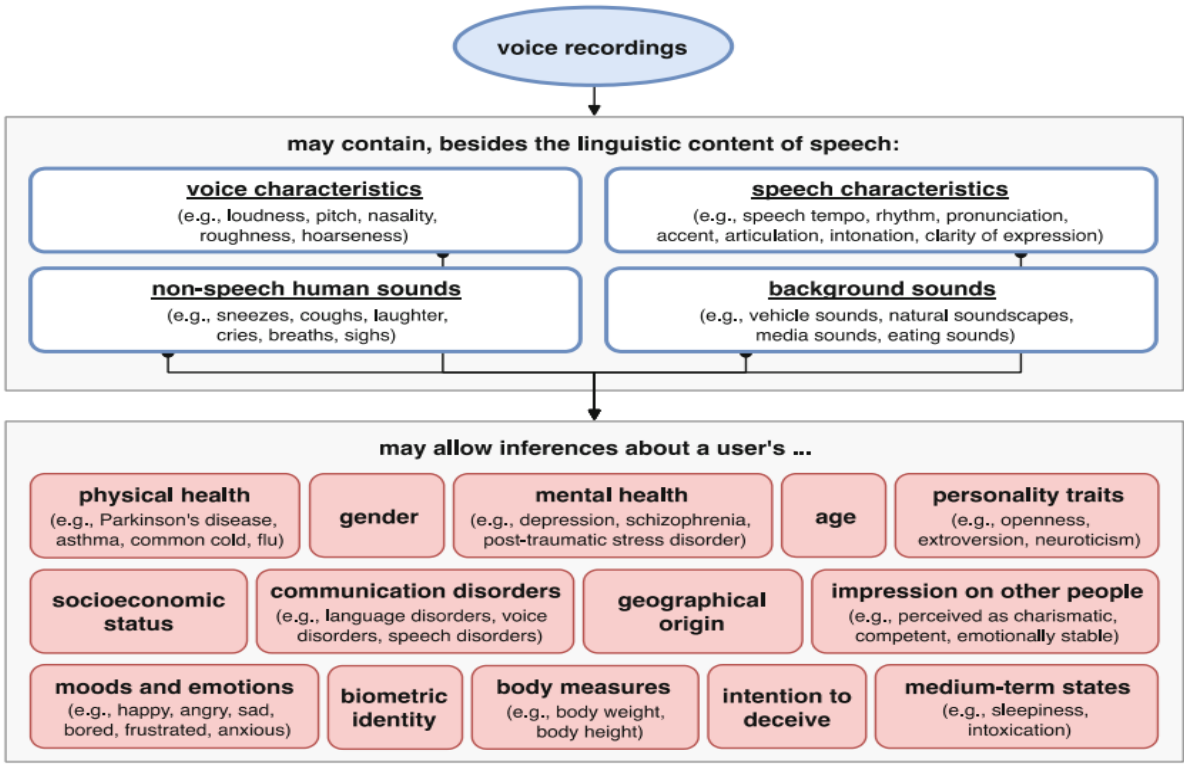


Source: Jacob Leon Kröger, Otto Hans-Martin Lutz and Florian Müller, 'What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking' in Michael Friedewald and others (eds), *Privacy and Identity Management. Data for Better Living: AI and Privacy* (Springer 2020).

Similarly, analysis of the speech and voice recognition technology that may be used to interact with these new devices can give companies insights into aspects of users' lives that they may not wish to divulge, such as their mood, personality traits, mental health, and state of mind (see Figure 4).[127] Evidently, this highly sensitive data is of tremendous value to corporations like Meta. Understanding the vices, triggers, and emotional state of their user base can inform marketing decisions and help tailor hyper-specific advertisements to individual users.

Figure 4. Inferences made from voice recordings

[127] Jacob Leon Kröger, Otto Hans-Martin Lutz and Philip Raschke, 'Privacy Implications of Voice and Speech Analysis – Information Disclosure by Inference' in Michael Friedewald, Melek Önen, Eva Lievens, Stephan Krenn and Samuel Fricker (eds), *Privacy and Identity Management. Data for Better Living: AI and Privacy*, (Springer 2020) <http://link.springer.com/10.1007/978-3-030-42504-3_16> accessed 26 June 2022.



Source: Jacob Leon Kröger, Otto Hans-Martin Lutz and Philip Raschke, 'Privacy Implications of Voice and Speech Analysis – Information Disclosure by Inference' in Michael Friedewald and others (eds), *Privacy and Identity Management. Data for Better Living: AI and Privacy*, (Springer 2020).

Emotional AI and soft biometrics are also increasingly being used by tech companies for targeted advertisement campaigns. Andrew McStay defines emotional AI as 'technologies that use affective computing and artificial intelligence techniques to sense, learn about and interact with human emotional life.'[128] This technology is powerful enough to detect depression and other health-related information about a person just from their image. While this presents clear medical benefits, experts have warned that the technology must be regulated to ensure valid consent is first obtained for this data to be used for marketing purposes, as existing data protection laws do not regulate emotional AI practices because the data is not 'legally personal,' i.e., it does not identify the individual.[129]

While these developments appear futuristic, Facebook is already exploiting users' privacy in similar ways on its social networking site. According to Cabañas and others, the company has labelled 73% of users within the EU, and 67% of users worldwide, with 'potentially sensitive interests' which may include their political opinions, sexual orientation, or personal health

[128] Andrew McStay, 'Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy' (2020) 7 Big Data & Society 1, 1.
[129] ibid, 4.

information.[130] Facebook obtains this data from 'likes' without the user's explicit consent and sells this information to advertisers, the ethical implications of which become evident in cases where Facebook infers that a person is interested in homosexuality in countries where this is a crime punishable by death. This puts the individual at considerable risk if their advertisements begin to reflect such an interest.[131] Moreover, Sandra Wachter has emphasized the discriminatory effects of affinity profiling - the grouping together of people based on assumed interests and using this information for financial gain. Facebook claims that this information does not infer ethnicity, sexual orientation, or other sensitive personal data, but rather one's 'affinity' with other groups based on the user's activity on the platform. Wachter argues that the grey area left behind by the GDPR, which does not regulate such indirect inferences, threatens users' freedom from discrimination.[132]

Nevertheless, the harvesting of instinctual and sensitive data in the background as one interacts naturally with friends and family in the metaverse goes far beyond the current practice of monitoring our active contributions such as likes and link clicks on the internet.[133] Furthermore, even if a user consents to the processing of his or her biometric data by accepting Meta's Terms and Conditions, it is unlikely that they will be properly and transparently informed of the extent to which this data can reveal information about their sexual orientation or harmful consumption habits.[134] In accordance with recital 60 of the GDPR, data subjects are to be made aware of the consequences of data profiling.[135] In a similar vein, recital 42 of the Regulation requires declarations of consent to be intelligible, easily accessible, and written in plain language.[136] Despite this, Meta has never been inclined to flaunt the consequences of its privacy-intrusive data profiling practices in its Terms of Service. This document is not designed to be read by users, instead it is long, abound with legal jargon, and hidden behind a link when signing up to the Facebook platform.[137] It is not in Meta's best interest to disclose its intensive and

[130] José González Cabañas, Àngel Cuevas, Aritz Arrate, Rubén Cuevas, 'Does Facebook Use Sensitive Data for Advertising Purposes?' (2021) 64(1) Communications of the ACM 62, 64.
[131] ibid.
[132] Sandra Wachter, 'Affinity Profiling and Discrimination by Association in Online Behavioural Advertising' (2020) 35(2) Berkeley Technology Law Journal 1 (forthcoming), 1.
[133] Norton Rose Fulbright 'The Metaverse: The Evolution of a Universal Digital Platform' (July 2021) <https://www.nortonrosefulbright.com/en/knowledge/publications/5cd471a1/the-metaverse-the-evolution-of-a-universal-digital-platform> accessed 5 May 2022.
[134] Javed Ahmed and others, 'GDPR Compliant Consent Driven Data Protection in Online Social Networks: A Blockchain-Based Approach,' (2020) 3rd International Conference on Information and Computer Technologies (ICICT), 307, 310.
[135] GDPR (n 51) recital 60.
[136] ibid, recital 42.
[137] Ahmed and others (n 134) 310.

exploitative data processing practices to the public as this may spawn public outcry and disincline users to sign up to the platform. This would hamper the company's primary goal which is to generate profits, upon which a functioning and effective ads-based business model is dependent. Additionally, the company will be even less inclined to disclose the fact the data collected from its metaverse hardware can essentially read its customer's minds and this information will be sold to marketers to develop even more privacy-intrusive advertisements. This poses a major threat not only to data subject rights but also to the right to privacy more broadly.

Biometric psychography and surveillance capitalism

Human rights lawyer and privacy advocate, Brittan Heller, has written extensively on the topic of biometric psychography, a term she coined to describe biometric information that is linked to a person's interests as opposed to their identity.[138] In 'The Problems with Immersive Advertising: In AR/VR, Nobody Knows You Are an Ad', written in conjunction with Avi Bar-Zeev, Heller emphasizes the fundamental difference between traditional billboard advertisements or even ads that appear in one's social media feed, and immersive reality in which a friend or relative's avatar could be used to recommend you buy a product or service - users will experience the metaverse from a first-person perspective, as opposed to the third-person perspective of the internet, which will render advertisements in XR inherently more personal.[139] This becomes even more worrisome in a Zuckerbergian metaverse where one interacts in a digitally rendered space with avatars that are virtually indistinguishable from reality. In this true-to-life digital environment, such hyper-targeted ads would essentially be irresistible to the individual.

If the practice of biometric psychography is left unregulated, the power and information asymmetry between large tech companies and the average consumer will lead to the creation of a closed metaverse that is built to generate large profits for the likes of GAFA, leaving individuals with little to no legal recourse to defend their right to data protection. These companies are currently operating within a legal vacuum that allows them to monopolise users' sensitive personal data for monetary gain.[140] Consequently, existing laws that did not foresee

[138] Heller (n 17) 15.
[139] Brittan Heller and Avi Bar-Zeev, 'The Problems with Immersive Advertising: In AR/VR, Nobody Knows You Are an Ad' (2021) 1(1) Journal of Online Trust and Safety 1, 9 <https://tsjournal.org/index.php/jots/article/view/21> accessed 7 May 2022.
[140] Kent Bye, State of Privacy in XR & Neuro-Tech: Conceptual Frames' (4 June 2021) 02:26 <https://www.youtube.com/watch?v=pIpD4-gYImU> accessed 6 May 2022.

the threats posed by emerging technologies must be updated to ensure the continued protection of the human right to privacy. More specifically, this will entail updating the definition of biometric data to include inferences made from those data that do not identify the individual. This will ensure that legislation such as the GDPR will continue to function as an essential tool for data protection in the metaverse due to the relatively high data privacy standards it sets and the vast portion of Meta's user base it protects.

On the other hand, some scholars proselytize that the combination of unchecked corporate power and the advent of the metaverse will usher in a new age of extended reality-driven surveillance capitalism.[141] This is a term that was coined by American author Shoshana Zuboff in her seminal book The Age of Surveillance Capitalism published in 2019. Zuboff describes this as an economic system that 'claims human experience as free raw material for hidden commercial practices of extractions, prediction, and sales.'[142] The competitive nature of such a market drives corporations to harvest ever-more accurate data in the pursuit of profits.[143] This pushes companies to use increasingly more invasive data collection methods to gain better insights into predicted consumer behaviour. The concentration of wealth, power, and knowledge in the hands of a few dominant players, means that individuals operating in a surveillance economy have little bargaining power to advocate for their own rights, sovereignty, and freedoms.[144]

Arguably, the metaverse is the apogee of surveillance capitalism as it will give the largest digital gatekeepers all-encompassing control over every aspect of our lives by recreating ourselves, our homes, and the wider world in a digital form that can be surveilled ubiquitously.[145] According to Zuboff's theory, the hunger to commodify more and more behavioural data to compete with the other incumbents will prevent these companies from complying with ethical norms around data protection, further encroaching on the right to privacy. This will lead to a dystopian, walled garden metaverse of the future that is centred around corporate interests as opposed to the user's experience. As pointed out by Kuzi Charamba, this potential for unprecedented concentration of corporate power calls for a

[141] Kuzi Charamba, 'Beyond the Corporate Responsibility to Respect in the Dawn of a Metaverse' (2022) University of Hong Kong Faculty of Law Research Paper No. 2022/14 1, 1 <http://dx.doi.org/10.2139/ssrn.4043254> accessed 6 May 2022.
[142] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019) definition.
[143] ibid.
[144] ibid.
[145] Charamba (n 141) 1.

reassessment of the UNGPs which merely place a moral obligation on corporations to respect human rights. Instead, Charamba argues that these principles should impose a corporate responsibility to respect and protect (positive obligation) digital human rights to better reflect the capabilities of advanced metaverse technologies.[146]

Freedom of Thought and the Right to Mental Privacy

In the context of this discussion on corporate surveillance through the use of biometric data, it is important to touch upon the potential for cognitive surveillance in the metaverse via BCI technologies, such as the wrist-based device Zuckerberg introduced at the 2021 Connect Conference. This device uses neural data to interpret what actions a person wishes to take – akin to reading the mind of the wearer.[147] In a recent talk at RightsCon 2022, engineer Dylan Urquidi highlighted the danger that neurotechnology such as this poses to freedom of thought.[148] Non-invasive brain-computer interface technologies that will soon enter the market entail huge potential for private companies like Meta to manipulate their user base and influence behaviours. Considering this, the ability to think thoughts privately and make choices freely could be under siege in an ever-more immersive metaverse.

In light of these developments, experts at The Neurorights Foundation are advocating for a common UN framework for the protection of neuro-rights and monitoring of the ethical development of neurotechnologies. This proposed framework is built upon the five following rights: the right to mental identity, the right to mental agency, the right to mental privacy, the right to fair access to mental augmentation, and protection from algorithmic bias.[149] Similarly, expert Kent Bye has argued that mental and biological privacy will be essential in the metaverse to ensure that our decisions continue to be made with integrity and not on the basis of external influences.[150] This highlights, yet again, the gaps that exist in the current regional and international human rights frameworks when it comes to the right to privacy and data protection.

---

[146] Ibid, 30.
[147] 'Inside Facebook Reality Labs: Wrist-Based Interaction for the next Computing Platform' (n 61).
[148] RightsCon 2022, 'Every breath you take, every move you make: neurotechnology, XR, and the metaverse of surveillance' (6 June 2022) 13:50 <https://rightscon.summit.tc/t/2022/events/every-breath-you-take-every-move-you-make-neurotechnology-xr-and-the-metaverse-of-surveillance-muemfgK7L82gzPRc7bPzGF> accessed 6 June 2022.
[149] Jared Genser, Stephanie Herrmann, and Rafael Yuste, *International Human Rights Protection Gaps in the Age of Neurotechnology* (NeuroRights Foundation 2022) 4-5.
[150] Takahashi (n 50).

Interim Conclusions

This chapter has attempted to outline the relevant ways in which Meta's vision for the metaverse infringes upon the right to data protection and, by extension, the right to privacy. It also touches upon freedom from discrimination in relation to emotional AI and threats to freedom of thought posed by neurotechnology. The GDPR is the most well-established piece of legislation that protects individuals from harmful and invasive data processing practices. Despite this, it appears to be in need of revision to tackle the new threats posed by immersive technologies. Namely, it must clarify the conditions for obtaining valid consent in the metaverse and move beyond a definition of biometric data that is linked exclusively to identify and recognise the 'legally personal' nature of inferences that can be made from such data. Furthermore, Heller's theory of biometric psychography begs additional questions about the international human rights framework, such as the extension of the right to privacy to cover mental privacy and the establishment of a corporate responsibility to protect human rights online. Either way, it is evident that updates to the regional and international legal framework that protects the right to privacy must happen quickly to keep step with Meta and prevent the emergence of a surveillance capitalism-driven digital future.

Chapter 3: Virtual Sexual Harassment Perpetrated Against Women and Children in the Metaverse

This chapter identifies digital sexual harassment as the primary way in which women and children's rights could be adversely affected in a Meta-led metaverse. I begin by detailing gaps in the current international human rights framework as it pertains to digital sexual harassment. I then focus on Codec Avatars as our digital twins in the metaverse and one of the primary forms through which we will interact with others. This warrants a discussion on the proteus effect and the phenomenon of avatar ownership. Research shows that users develop a close connection with realistic avatars, which will be enhanced by verisimilitude and 'social presence' in the metaverse. On the other hand, this will have major implications for the mental health of users whose avatars are discriminated against and threatened or abused by others. Therefore, I posit the growing trend in favour of data ownership as a potential solution to this ethical quandary. Finally, a select few cases of sexual harassment in social VR, including of children, are presented in order to demonstrate the pervasiveness of this phenomenon and contemporary attitudes towards sexual harassment that is perpetrated in digital environments. It is evident that further steps need to be taken to protect the rights of women and children in the metaverse, which should be set in motion by the legal recognition of sexual harassment in the metaverse.

Gender-based Violence in International Law

Over time, major international and regional human rights institutions have recognised the need to protect women from online abuse in digital environments. This typically takes the form of online sexual harassment which is considered to contribute to gender-based violence in the physical world. This new phenomenon is pervasive, as was illustrated by a 2015 study conducted by UNESCO which revealed that 73% of women have experienced or been exposed to some form of violence online.[151] There is also an intersectional dimension to this form of digital gender-based violence, with Black women being 84% more likely to be the targets of abusive messages on Twitter, according to Amnesty International.[152] Similarly, female members of the LGBTQ+ community and women with disabilities are more likely to be on the

[151] UN Broadband Commission for Digital Development Working Group on Broadband and Gender, '*Cyber Violence Against Women and Girls: A World-Wide Wake Up Call'* (23 October 2015) <https://en.unesco.org/sites/default/files/genderreport2015final.pdf> accessed 12 May 2022, 2.
[152] Amnesty International, 'Troll Patrol Findings: Using Crowdsourcing, Data Science & Machine Learning to Measure Violence and Abuse against Women on Twitter' <https://decoders.amnesty.org/projects/troll-patrol/findings> accessed 12 May 2022.

receiving end of online hate.[153] This has created a scenario in which women do not feel safe in digital spaces; this is particularly true for female public figures such as politicians, journalists, and human rights defenders who face an increased level of abuse and threats online, often from anonymous profiles.[154] Additionally, this has a detrimental and disempowering impact on women and their ability to exercise their fundamental rights and freedoms such as freedom from discrimination, freedom of expression, and the right to private life.

However, the Convention on the Elimination of All Forms of Discrimination against Women adopted by the UN in 1979 makes no mention of either gender-based violence or violence against women.[155] Gender-based violence was first recognised as a form of discrimination against women in general recommendation no. 19 to the Convention.[156] Subsequently, general recommendation no. 35, which was concluded in 2017, finally acknowledged the need for relevant stakeholders to take the necessary measures to prevent gender-based violence in digital environments.[157] However, these general recommendations are not legally binding, leaving numerous gaps in the international human rights framework to tackle online harassment of women and girls.

In the context of this porous and inadequate global framework, the treaty-making power of the Council of Europe has proven more effective in protecting the rights of women online. Also known as the Convention on Preventing and Combatting Violence against Women and Domestic Violence, the Council of Europe has described the Istanbul Convention as 'the most far-reaching legal instrument to prevent and combat violence against women and domestic violence.'[158] However, it has been criticised for only indirectly applying to violence perpetrated against women online.[159] In recognition of this legislative gap, GREVIO adopted general

[153] Amnesty International, 'Toxic Twitter - Triggers of Violence and Abuse Against Women on Twitter' <https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women-chapter-2/> accessed 12 May 2022.
[154] Dunja Mijatović, 'No Space for Violence against Women and Girls in the Digital World' (*Council of Europe Portal*, 15 March 2022) <https://www.coe.int/en/web/commissioner/blog/-/asset_publisher/xZ32OPEoxOkq/content/no-space-for-violence-against-women-and-girls-in-the-digital-world> accessed 12 May 2022.
[155] Convention on the Elimination of All Forms of Discrimination Against Women (adopted 13 December 1979, entered into force 3 September 1981) 1249 UNTS 13 (CEDAW).
[156] UN Committee on the Elimination of Discrimination Against Women, 'General Recommendation No 19 of CEDAW on Violence Against Women (11th session, 1992), UN Doc HRI/Gen/1/Rev.6, para 1.
[157] UN Committee on the Elimination of All Forms of Violence Against Women, 'General Recommendation No 35 on gender-based violence against women, updating general recommendation No. 19 (2017) UN Doc C/GC/35, para 20.
[158] Mijatović (n 154).
[159] Sara de Vido, 'The Istanbul Convention and Its Impact on EU Law and Policies' Ca' Foscari University of Venice (Trier, 20 November 2018).

recommendation no. 1 to the Convention in October of 2021 which pertains to the digital dimension of violence against women. The document addresses the issue in its three most prominent forms – online sexual harassment, online and technology-facilitated stalking, and the digital dimension of psychological violence.[160] The case law of the European Court of Human Rights further confirms the responsibility of states to protect women and girls from gender-based violence in digital spaces. For example, the Court's ruling in the 2021 case of Volodina vs. Russia held that the state had failed to protect the applicant against repeated acts of cyberviolence perpetrated by her former partner.[161]

From this brief overview, one can observe that states have only recently begun to recognize the need to protect women from online harassment. This is rather worrisome when one considers the speed at which new technologies are developing. Meta envisions millions of users interacting in AR, VR, and MR environments for extended periods of time within the next decade.[162] With these innovations come new threats to the safety of women and girls. This begs the question of whether the existing international human rights framework is capable of protecting women from sexual harassment in the metaverse. If not, by what other legal means can this problem be addressed?

Identity and the Proteus Effect in the Metaverse

A 2019 study conducted by Blackwell and others found that women, children, people of colour, and those without 'American' accents were the most common targets of harassment in VR. This was the case despite the VR games included in the study only offering cartoon-like avatars that reveal limited information about a user's identity.[163] Therefore, Facebook Reality Lab's photorealistic Codec Avatars will not only be inextricably linked to our own identities and self-perception but will also make it impossible for users to disguise cues, such as gender and race, that may render them targets for virtual abuse. In addition to this, despite the limited avatar selection associated with traditional video games, researchers have observed that certain characteristics associated with one's digital representation have important psychological impacts and can alter real world behaviour.[164] This phenomenon has been dubbed the 'proteus

[160] Group of Experts on Action against Violence against Women and Domestic Violence 'GREVIO General Recommendation No. 1 on the Digital Dimension of Violence against Women' (adopted 20 October 2021).
[161] For example, see *Volodina v Russia* (no. 2) App no 40419/19 (ECtHR, 14 September 2021).
[162] Heath (n 2).
[163] Lindsay Blackwell and others, 'Harassment in Social Virtual Reality: Challenges for Platform Governance' (2019) 3 Proceedings of the ACM on Human-Computer Interaction 1, 13.
[164] Nick Yee and Jeremy Bailenson, 'The Proteus Effect: The Effect of Transformed Self-Representation on Behavior' (2007) 33 Human Communication Research 271.

effect' and it can have wide-ranging societal implications, for better or worse. For example, a 2007 study conducted by Nick Yee and Jeremy Bailenson showed that people who were assigned more attractive avatars were more confident in approaching members of the other sex and were more willing to share information about themselves. A similar boost in confidence levels was observed in participants who had taller avatars.[165] Furthermore, a 2017 experiment conducted by Tabitha Peck and others allocated avatars of a darker skin colour to sixty participants. The results of the experiment were twofold: first, it revealed that immersive virtual reality gave the participants the illusion of ownership over their avatars, and second it demonstrated that embodiment in a darker-skinned avatar reduced implicit racial bias among participants, at least temporarily.[166]

It remains to be seen how the proteus effect will manifest itself in a metaverse where our surroundings and avatars are virtually indistinguishable from the real world. Despite some observed positive effects of the proteus effect, representations in the form of Codec Avatars may not bode well for women and other marginalized groups in society. Tany Basu has highlighted the adverse impact this may have on young women experiencing body dysmorphia.[167] In a 2021 study conducted by Jennifer Ogle, eighteen women who were identified as struggling with body image concerns visited a research lab where a 3D virtual avatar of their likeness was created. Half of the participants participated in a body positivity programme before the avatar creation process, while the other half did not. The results of the study indicated that, in some cases, regardless of whether they had taken part in the body positivity programme or not, the virtual avatar experience harmed participant's body image.[168] Similar harms may be caused to the mental health of trans people whose physical appearance may not yet reflect their true identity.[169]

Beyond body dysmorphia and gender dysphoria, presenting as a faithful version of one's real self in the metaverse may cause unintended harm for those members of society who are the targets of online abuse based on their gender, race, or sexual orientation. For example, many

---

[165] Ibid, 285.
[166] Tabitha C. Peck and others, 'Putting Yourself in the Skin of a Black Avatar Reduces Implicit Racial Bias' (2013) 22(3) Consciousness and Cognition 779, 784.
[167] Tany Basu, 'The Metaverse Is the next Venue for Body Dysmorphia Online' *MIT Technology Review* (16 November 2021) <https://www.technologyreview.com/2021/11/16/1040174/facebook-metaverse-body-dysmorphia/> accessed 14 May 2022.
[168] Juyeon Park and Jennifer P. Ogle, 'How virtual avatar experience interplays with self-concepts: the use of anthropometric 3D body models in the visual stimulation process' (2021) 8(28) Fash Text 1, 16 <https://doi.org/10.1186/s40691-021-00257-6> accessed 14 May 2022.
[169] Basu (n 167).

female players of World of Warcraft avoid choosing female avatars on account of the abuse these avatars receive from other players relative to male avatars. Female avatars are hyper-sexualized in the game which leads to players receiving unsolicited and inappropriate messages.[170] In addition to this, a recent survey conducted by Reach3 Insights revealed that 59% of women avoid presenting as female in online video games, meaning they choose male or non-gendered avatars, to avoid sexual harassment.[171] This has created a scenario where women often perceive themselves to be unwelcome and unsafe in digital environments.

Business Insider has also reported that sexual harassment can be worse and occur more frequently online than in the real world as players feel emboldened by the anonymity afforded to them in a video game, as opposed to the physical world where there is at least some recognition of accountability for one's actions.[172] If the necessary safeguards are not put in place from the outset, this problem will only see exponential growth in the metaverse. Considering that sexual harassment has already been well documented in online video games and social VR environments, Meta must recognise the harms that Codec Avatars pose to women's rights. Subsequently, it must not knowingly lead them into such distressing and harmful situations under the guise of it being a virtual utopia in which anything is possible.

Immersive VR as an Amplifier of Traumatic Responses to Virtual Sexual Harassment

The ownership that one is likely to feel over their photorealistic Codec Avatar will be enhanced by the immersive nature of metaverse technologies. Zuckerberg believes that 'social presence' is imperative to creating a metaverse that feels real and believable.[173] This will be achieved through immersive VR technologies, such as Project Cambria, which give the user the impression that they are really 'in' the metaverse. In an interview with Brittan Heller, VR researcher Jessica Outlaw described the feeling of presence in immersive virtual reality:

> '[W]hen I'm in a VR headset and I talk to people I know, I actually have the sense of being there with them and having an embodied experience…I create memories with

[170] Jaigris Hodson and Pamela Livingstone, 'View of Playing in Drag: A Study on Gender In Virtual and Non-Virtual Gaming' (2017) 10(16) The Journal of the Canadian Game Studies Association 109, 111 <https://journals.sfu.ca/loading/index.php/loading/article/view/182/209https://journals.sfu.ca/loading/index.php/loading/article/view/182> accessed 14 May 2022.
[171] Reach3 Insights, 'Reach3 Insights' New Research Reveals 59% of Women Surveyed Use a Non-Gendered/Male Identity to Avoid Harassment While Gaming' (19 May 2021) <https://www.reach3insights.com/women-gaming-study> accessed 16 May 2022.
[172] Antonio Villas-Boas, 'Scientists Looked at How Ugly Avatars Are Treated Compared to Hot Ones and Found an Unfortunate Truth' *Business Insider* (7 May 2015) <https://www.businessinsider.com/how-good-your-avatar-looks-has-a-negative-impact-2015-5> accessed 14 May 2022.
[173] Meta (n 7) 06:33.

them in these virtual environments…I don't feel like there's a huge difference between hanging out with my friends in a virtual space compared to hanging out with them in the actual physical world.'[174]

According to emerging research, this verisimilitude creates a close connection between users and their avatars. Guo Freeman and others recently conducted a study of thirty participants which revealed that the direct connection between a user's body and their avatar in social VR led to them feeling a stronger affinity with their avatars than they did in traditional online gaming. Furthermore, some participants reported feeling as though their avatars were extensions of themselves. Another participant noted that because their avatar moved in unison with their own body movements, the virtually rendered experience could be mistaken for real life.[175] This finding is confirmed by emerging research which suggests that verisimilitude in VR deceives the brain into registering virtual experiences as real. In Lemley and Volokh's 'Law, Virtual Reality, and Augmented Reality' the authors claim that users can feel 'scared to death' by a realistic game in VR, even if they are not harmed physically.[176] This is because the brain responds with the same neural reaction as though the activity were being carried out physically. This goes far beyond the psychological impact of online video games that the brain understands to be observing in the third person.[177]

It is important to consider the findings of this research in the context of sexual harassment in social VR. It suggests that the brain will interpret virtual sexual harassment perpetrated against our avatars in the same way it would if the crime were committed in the physical world. This means that the victim will suffer the same psychological harm and traumatic response. To this point, philosopher David J Chalmers has added that harassment in the metaverse will be more traumatic than the verbal harassment often directed at women on social media, due to the 'embodiment' aspect of immersive technologies.[178] The effects of sexual harassment in the

[174] Heller (n17) 8.
[175] Guo Freeman and others, 'My Body, My Avatar: How People Perceive Their Avatars in Social Virtual Reality' (2020) Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems, 4-5 <https://dl.acm.org/doi/10.1145/3334480.3382923> accessed 14 May 2022.
[176] Mark Lemley and Eugene Volokh, 'Law, Virtual Reality, and Augmented Reality' (2018) 166(5) U. PA. L. REV 1051, 1066.
[177] ibid.
[178] Laurie Clarke, 'Can We Create a Moral Metaverse?' *The Guardian* (14 May 2022) <https://www.theguardian.com/technology/2022/may/14/can-we-create-a-moral-metaverse> accessed 3 July 2022.

metaverse will be further compounded by advances in haptic technology, such as haptic gloves, suits, and clothing, that simulate the feeling of touch.[179]

In light of these issues surrounding avatars, immersive technologies, and user interactions in the metaverse, a growing body of literature is advocating for the user's right to ownership over their digital twins in Web 3.0, or at least the data that is used to build them.[180] For example, Heather Vescent has argued that a user-centric approach to digital identities in the metaverse could prevent the misuse of personal data and empower the user to take control over their digital lives.[181] Similarly, Olga Mack asserts that digital twins are born out of the fruits of our own labour and are, thus, extensions of our physical selves that we will grow closer to the more time we spend in the metaverse.[182] This paper has already determined that Codec Avatars will serve as our digital twins in the metaverse. They will use biometric data, such as skin tone, hair texture, and eye colour, to create exact replicas of real people. These avatars will mirror our facial expressions, hand gestures, and body posture with the help of a full-body scan and 360-degree surveillance.[183] They can also be updated to reflect changes in our appearance, such as the addition of new tattoos, a new haircut, or a shaved beard.[184] Consequently, it is not inconceivable to suggest that they will become extensions of ourselves and that we will develop a sense of ownership over them. This makes it imperative that they are also protected from harm in order to respect the mental health and dignity of their real-world human equivalents.

Considering this, the personality theory that is associated with intellectual property law suggests that the author of a work forms an emotional bond with his or her creation since it is a manifestation of the individual's own personality. Therefore, moral rights should be bestowed upon the author to protect the integrity of the work and the dignity of its creator.[185] Meta's digital twin avatars will look and act exactly like us because they will be built using our own personal data which requires a certain degree of effort and creativity on behalf of the user. For

[179] eSafety Commissioner, 'Immersive Technologies – Position Statement' (10 December 202) <https://www.esafety.gov.au/industry/tech-trends-and-challenges/immersive-tech> accessed 15 May 2022.
[180] Olga V. Mack, 'Who Owns Your Digital Twin? Not You—and Here's Why That's a Massive Problem | Opinion' *Newsweek* (1 August 2019) <https://www.newsweek.com/who-owns-your-digital-twin-not-you-heres-why-thats-massive-problem-opinion-1451991> accessed 3 July 2022.
[181] Heather Vescent, 'The Metaverse: A Missed Opportunity for Data Ownership and Privacy?' *Biometric Update* (21 January 2022) <https://www.biometricupdate.com/202201/the-metaverse-a-missed-opportunity-for-data-ownership-and-privacy> accessed 3 July 2022.
[182] Olga V. Mack (n 180).
[183] 'Facebook Is Building the Future of Connection with Lifelike Avatars' (n 68).
[184] Meta (n 7) 1:03:10.
[185] The Berkman Klein Center for Internet & Society, 'William Fisher, CopyrightX: Lecture 2.1, Fairness and Personality Theories: Introduction' (16 January 2015) <https://www.youtube.com/watch?v=nKyWusznRgQ> accessed 14 May 2022.

this reason, individual users could be considered authors of their own Codec Avatars in accordance with IP law. This would give the user greater control over how their avatar and personal data are used and afford them greater options for legal recourse in the face of external threats.[186]

However, legal ownership over personal data/ metaverse avatars alone is not enough to prevent the virtual sexual harassment that has become commonplace in social VR, such as Facebook's Horizon Worlds. Meanwhile, the safety mechanisms the platform has put in place appear to be absent or ineffectual, with Meta often placing the blame on victims for not deploying them correctly.[187] Thus, the law should eventually evolve to recognise the legal personality of avatars to allow them to be sued or prosecuted for virtual crimes, including sexual harassment, that are committed in the metaverse.[188] Moreover, laws pertaining to sexual harassment must be updated to coincide with the threats posed by cutting-edge metaverse technologies. This must be accompanied by changes in societal attitudes to recognise that the trauma resulting from sexual harassment in immersive VR is akin to physical reality. If these changes are not made promptly, then it will culminate in a metaverse that is hostile and discriminatory towards women.

The Experiences of Women and Girls in Social Virtual Reality to Date

Incidents of sexual harassment

The following section details the encounters that three female researchers have had with sexual harassment in social virtual reality. It also highlights how these women have been demeaned in their attempts to expose the disturbing behaviour of certain actors in social VR. As it stands, the public attitude towards virtual sexual harassment is that it is not on par with sexual harassment in the physical world. This sets a dangerous precedent for the metaverse and may hamper women's' ability to enjoy the benefits that such advanced technologies have to offer.

Metaverse researcher, Nina Jane Patel, recently documented her experience in Horizon Venues, the virtual reality events platform created by Meta's Oculus Quest that will soon be merged

[186] Vescent (n 181).
[187] Pin Lean Lau, 'An Ecosystem of Interconnectedness: Prioritising Key Legal Concerns in the Metaverse' *The World Financial Review* (25 May 2022) <https://worldfinancialreview.com/an-ecosystem-of-interconnectedness-prioritising-key-legal-concerns-in-the-metaverse/> accessed 3 July 2022.
[188] Ben C. Cheong, 'Avatars in the metaverse: potential legal issues and remedies' (2022) Int. Cybersecur. Law Rev. <https://doi.org/10.1365/s43439-022-00056-9> accessed 3 July 2022.

into Horizon Worlds.[189] Zuckerberg has described Horizon Worlds as 'core to our metaverse vision' and the platform is rapidly gaining in popularity having recently hit 300,000 users.[190] However, upon entering the platform Patel recalls being bombarded by male avatars who began to grope her. When she tried to escape by moving away, they pursued her while shouting 'Don't pretend you didn't love it; this is why you came here.'[191] Eventually, she removed her headset to escape the abusers. Patel reported that the abuse had happened so quickly that she did not have a chance to enact any of the available safety features.[192] The same article highlighted recent research conducted by the Centre for Countering Digital Hate which found 100 potential violations of Meta's social virtual reality policies in the space of 11 hours and 30 minutes. This amounted to one act of abusive behaviour, including sexual harassment, every seven minutes, which contradicts Zuckerberg's promises in October of 2021 to prioritise privacy and safety in the metaverse from the outset.[193]

In 2016, a similar experience was reported by a researcher and author operating under the pseudonym Jordan Belamire while playing the virtual reality game QuiVr. In this game, the user assumes the avatar of an archer who must shoot down the advancing enemy. As soon as Belamire identified herself as female by using the voice function, another player began to make rubbing motions on her chest. After she told him to stop and turned to move away, he followed her, grabbing and pinching at her chest area and rubbing his hand on her virtual crotch.[194] It is important to note that avatars in QuiVr appear only as a floating helmet, quiver, and two floating hands, one that is always holding a bow and the other that is free (see Figure 5). Therefore, when Belamire reported that the player was rubbing her chest and crotch, he was using his free hand to make inappropriate gestures in those general areas. Despite this, she

[189] Scott Hayden, 'Meta to Merge "Venues" Event Space into "Horizon Worlds" Social VR Platform' *Road to VR* (9 May 2022) <https://www.roadtovr.com/meta-venues-events-horizon-worlds-quest-2/> accessed 15 May 2022.
[190] Alex Heath, 'Meta's Social VR Platform Horizon Hits 300,000 Users' The Verge (17 February 2022) <https://www.theverge.com/2022/2/17/22939297/meta-social-vr-platform-horizon-300000-users> accessed 11 June 2022.
[191] Olivia Petter, 'Why Is No One Taking Sexual Harassment In The Metaverse Seriously?' *British Vogue* (20 March 2022) <https://www.vogue.co.uk/arts-and-lifestyle/article/sexual-assault-in-the-metaverse> accessed 15 May 2022.
[192] ibid.
[193] Center for Countering Digital Hate, 'Facebook's Metaverse Is Unsafe' *CCDH* (30 December 2021) <https://www.counterhate.com/metaverse> accessed 15 May 2022.
[194] Jordan Belamire, 'My First Virtual Reality Groping' *Athena Talks* (22 October 2016) <https://medium.com/athena-talks/my-first-virtual-reality-sexual-assault-2330410b62ee> accessed 15 May 2022.

claimed that the virtual abuse felt just as real and scary as though it had happened in the real world.[195]

Figure 5. QuiVr Avatar

Source: Jordan Belamire, 'My First Virtual Reality Groping' *Athena Talks* (22 October 2016) <https://medium.com/athena-talks/my-first-virtual-reality-sexual-assault-2330410b62ee> accessed 15 May 2022.

Similar to Patel's situation, when Belamire shared her negative experience in QuiVR online she was not met with an entirely positive response, with one commenter stating:

> 'Calling this sexual assault is disrespectful to actual victims of sexual assault. You where a victim of unpleasant harassment, bad behaviour and someone waving virtual controllers in a rather slimey manner but you where not and never where a victim of sexual assault. It's the equivalent of arguing that you where a victim of virtual murder because someone shot you in a VR computer game.'[196]

This individual is referring to the fact that Belamire described her experience as sexual assault which requires an 'actus reus', or physical element, that was lacking in this case.[197] Additionally, because the harm done to the victim is psychological and not physical, it is

[195] ibid.
[196] ibid.
[197] Richard Wee, Fatin Ismail and Kimberly Chan, 'The Metaverse and Its Legal Issues' Richard Wee Chambers (18 February 2022) <https://www.richardweechambers.com/the-metaverse-and-its-legal-issues/> accessed 1 June 2022.

difficult to prove that a sexual assault has occurred.[198] On the other hand, sexual harassment does not require physical contact to constitute a crime, yet women who have recounted such experiences in social VR have been met with similarly demeaning responses. For example, when Patel first wrote about her experience with sexual harassment in Horizon Venues on Facebook, an individual commented on her post to say: 'don't be stupid, it wasn't real.'[199] This dismissive attitude has also been encountered by Jessica Outlaw during her research into harassment in social VR. Several respondents to a survey she conducted in 2018 questioned the very existence of harassment in social VR with one user responding 'Oh grow up. It's pixels on a screen.'[200] This attitude has important social implications for women as it suggests that they simply shrug off the incessant abuse they will face in the metaverse and refrain from sharing their experiences. Not only does enable the perpetrators of abuse, but it may also encourage this behaviour to be replicated in the real world as per the Proteus effect.

The experiences of Patel and Belamire were not unique or isolated events. Outlaw's 2018 survey found that 49% of female respondents had experienced sexual harassment in social VR environments.[201] Evidently, some users see the metaverse as a utopia in which they can act out their 'darkest urges.'[202] These bad actors have interpreted the limitless and lawless nature of virtual worlds as permission to violate others without facing legal consequences, benefitting from the popular belief that virtual reality is not real and no true harm is being caused. From an ethical standpoint, the developers of metaverse technologies must be cognizant of the toll this discriminatory environment will take on the mental and psychological health of women and girls and implement the necessary prevention and harm-reduction measures.

In 2016, American journalist Taylor Lorenz publicised her experiences with inappropriate behaviour using the social VR app Altspace. Within minutes of entering the space, Lorenz was approached by other users who began to make rubbing gestures toward her avatar and asked if she was this 'skinny in real life.'[203] After her story garnered media attention, many social VR platforms introduced new mechanisms to protect one's personal space. For example, Altspace

[198] Blackwell and others (n 163) 14.
[199] Petter (n 191).
[200] Jessica Outlaw, 'Virtual Harassment: The Social Experience of 600+ Regular Virtual Reality (VR) Users' *Medium* (5 April 2018) <https://virtualrealitypop.com/virtual-harassment-the-social-experience-of-600-regular-virtual-reality-vr-users-23b1b4ef884e> accessed 15 May 2022.
[201] ibid.
[202] Susan W. Brenner, 'Fantasy Crime: The Role of Criminal Law in Virtual Worlds' (2008) 11(1) Vanderbilt Journal of Entertainment and Technology Law 1, 95.
[203] Taylor Lorenz, 'Virtual Reality Is Full of Assholes Who Sexually Harass Me. Here's Why I Keep Going Back' *Mic* (26 May 2016) <https://www.mic.com/articles/144470/sexual-harassment-in-virtual-reality> accessed 15 May 2022.

has introduced a blocking feature that makes your avatar invisible to others. The platform also takes measures to suspend or terminate the accounts of users reported for bullying and harassment.[204] With regards to Facebook Horizon, virtual reality designers Michelle Cortese and Andrea Zeller have been tasked with incorporating the idea of consent into the platform. One manifestation of this is a button that a user can press to immediately remove themselves from a social setting.[205] Facebook has also added a 'personal boundary' feature to Horizon Worlds and Horizon Venues which creates a two-meter personal bubble around an avatar to prevent other players from entering that space.[206]

While it is encouraging that platforms are taking steps to address sexual harassment, the measures that have been implemented thus far focus more on protecting the individual than punishing the abuser. Hence, they can be seen only as interim, reactionary, and ineffective in tackling the structural issues that allow this behaviour to proliferate. In a 2008 journal article, Susan W. Brenner predicted that there would soon come a time when crimes that were committed in the virtual world would require the application of criminal law.[207] Arguably, the advent of the metaverse as an alternate digital realm that is closely intertwined with our physical world signifies that this time has come. Of the four legal elements that constitute a crime (actus reus, mens rea, causation, and harm), scholars have traditionally struggled to prove that virtual sexual crimes cause harm.[208] However, through existing research and witness accounts, this chapter has attempted to show the adverse psychological effects such crimes can have if perpetrated in an immersive metaverse against a digital twin avatar. Therefore, laws relating to sexual harassment, assault, and rape, should be applied to the metaverse to reflect the seriousness of this issue. However, this will certainly raise questions of legal jurisdiction, the legal accountability of platforms, and the appropriate punishment for virtual crimes that are beyond the scope of this paper.

Incidents of child grooming

It is also necessary to touch briefly upon the growing issue of child grooming in social VR as children will inevitably be the earliest adopters of Zuckerberg's metaverse. Meta's Oculus

[204] ibid.
[205] Michelle Cortese, 'Designing Safer Social VR' *Medium* (19 November 2019) <https://immerse.news/designing-safer-social-vr-76f99f0be82e> accessed 16 May 2022.
[206] 'Metaverse Is Already Limiting Virtual Sexual Assault' *Verdict* (11 February 2022) <https://www.verdict.co.uk/metaverse-meta-sexual-assault/> accessed 16 May 2022.
[207] Brenner (n 202) 94.
[208] Ibid, 2.

Quest VR headset was the most popular Christmas gift in 2019.[209] Meanwhile, the Oculus virtual reality app was the most downloaded app in the App Store on Christmas Day in 2021.[210] This may explain why users of Horizon Worlds with an age limit of 18+ commonly complain about foul-mouthed children using the platform and ruining the experience for others.[211] In addition to this, emerging research has shown how easily children can be exposed to inappropriate behaviour, grooming, and sexual harassment in social VR environments. For example, a researcher from the UK recently reported experiencing grooming, racism, and rape threats when posing as a 13-year-old girl in the virtual world VRChat which can be accessed through an Oculus VR headset.[212] According to XRSI's child safety initiative, children under the age of 13 should not be using VR and teenagers should only have restricted access.[213] As demonstrated by the case of Horizon Worlds, this is difficult to enforce and does not solve the issue of children over the minimum age limit being exposed to inappropriate and dangerous content. Moreover, it is difficult for parents to observe the actions of children in VR as not every user has access to an external display monitor.[214]

Moreover, in an internal company memo last year, Andrew Bosworth, Chief Technology Officer at Meta, wrote that moderating the speech and actions of users in the metaverse 'at any meaningful scale is practically impossible.'[215] Considering that the company has already failed on numerous occasions to monitor harmful content on social media, there is a risk that a Meta-dominated metaverse will become a breeding ground for hate speech, extremism, and sexual harassment, particularly directed at women, children, and people of colour. The immersive nature of XR will render these experiences more traumatic for the victims. As a consequence of this, Charamba's argument in favour of a corporate responsibility to protect presents itself

[209] Travis Hoium, 'Oculus Devices Sold Out in a Positive Sign for Virtual Reality' *The Motley Fool* (27 December 2019) <https://www.fool.com/investing/2019/12/27/oculus-devices-sold-out-in-positive-sign-for-virtu.aspx> (accessed 11 June 2022).
[210] Steve Kovach, 'How the Metaverse Won Christmas' CNBC (27 December 2021) <https://www.cnbc.com/2021/12/27/metas-oculus-virtual-reality-headsets-were-a-popular-holiday-gift.html> accessed 11 June 2022.
[211] Will Oremus, 'Kids Are Flocking to Facebook's "Metaverse." Experts Worry Predators Will Follow.' *Washington Post* (7 February 2022) <https://www.washingtonpost.com/technology/2022/02/07/facebook-metaverse-horizon-worlds-kids-safety/> accessed 6 July 2022.
[212] 'Undercover Journalist Witnesses Abuse in Metaverse' *BBC News* (23 February 2022) <https://www.bbc.com/news/av/uk-60466557> accessed 11 June 2022.
[213] XRSI, 'The Child Safety Initiative' <https://xrsi.org/programs/child-safety> accessed 3 July 2022.
[214] Oremus (n 211).
[215] Hannah Murphy, 'How Will Facebook Keep Its Metaverse Safe for Users?' *Financial Times* (12 November 2021) < https://www.ft.com/content/d72145b7-5e44-446a-819c-51d67c5471cf> accessed June 11 2022.

again as a more favourable alternative to relying on the good faith of Meta to defend human rights in the metaverse.[216]

Interim Conclusions

Meta wishes to generate realistic social presence in the metaverse, which will require users to develop a close personal connection with their digital twin avatars. However, this also creates perilous conditions for the mental health of users who will experience harassment and assault in the metaverse. Although the prevalence of digital gender-based violence has been well-documented for several years, many human rights institutions have not yet recognised its potential impact on society. Furthermore, the widely held belief among Meta's userbase that acts perpetrated in the metaverse are 'not real' will result in an environment that is inhospitable for women, children, and people of colour. Hence, this chapter identifies several legal interventions to mitigate these potential harms. First, property law shows promise in advancing the Web 3.0 trend of data sovereignty and legal ownership over personal data could give users more control over their avatar's privacy. Second, legislative reforms are required to clarify the definition of and criteria for sexual crimes such as assault and rape that are perpetrated in the metaverse. Lastly, including a corporate responsibility to protect in the UNGPs would compel Meta to effectively moderate harmful content on its metaverse platforms. If these reforms come too late it will hinder the ability of many women and children to peacefully enjoy their right to privacy, freedom of expression, and freedom from discrimination in the future.

[216] Charamba (n 141).

Chapter 4: Recommendations for Metaverse Governance

The aim of this paper is not to promote anti-innovation bias but rather to ensure that the benefits of such innovation are enjoyed by the many and not the few. In doing so, this paper has brought a human rights perspective to the bleeding edge of Web 3.0 technology, a place where it is often absent. In line with research question three, four distinct yet highly interconnected themes have emerged throughout this analysis of the human rights implications and legal issues arising from Meta's metaverse ambitions: (1) consider the economic incentives at play; (2) mandate the prioritisation of UX/UI design; (3) rectify the identified legal considerations, and (4) consider the broader socio-ethical implications. Policymakers and lawmakers should consider these four aspects when designing regulation to ensure the metaverse remains human rights compliant and not solely profitable. These four elements are summarized Table 2 in below.

Table 2. Recommendations for Metaverse Governance

Recommendation	Major Concerns	Impacts for metaverse
Consider the economic incentives at play	Prioritisation of profit over public interest, anti-competitive practices	Lack of interoperability, closed platforms, exploitation of user data
Mandate the prioritisation of UX/UI design	Non-implementation of privacy, security, and safety by design principles, users unaware of their rights	Lack of consumer privacy and safety, especially with regards to children, predatory advertising
Rectify the identified legal issues	Web 3.0 inherits the unsolved issues of Web 2.0, retrofitted or reactionary legislation	The metaverse becomes a legal 'wild west' with potential for widespread human rights abuse
Consider the broader socio-ethical implications	Exacerbation of the digital divide, unintended harms for marginalised groups, deterioration of users' mental health	Bias is coded into new metaverse technologies

Consider the Economic Incentives at Play

Policymakers must be cognizant of the economic incentives driving the push for the metaverse. Corporations like Meta are driven by a need to grow and generate greater profits year on year. Some authors have argued that this is the true reason behind the company's major rebrand in October of 2021. As Alex Health argues, if Meta can regain the interest of young people who have migrated from Facebook and Instagram in recent years, then it can secure a profitable

future in this new digital frontier known as the metaverse.[217] Moreover, economic incentives may also explain Meta's stringent focus on developing AR/VR hardware devices as opposed to the interoperable infrastructure necessary to create the metaverse. Heath has pointed to the company's frustration with being at the mercy of their competitors Apple and Google who can dictate the rules applied to apps like Facebook, Instagram, and WhatsApp. In the past, these companies have hurt Meta's ads-based business strategy by introducing new regulations, such as stricter data transparency requirements.[218] Therefore, Meta's new hardware devices such as Project Nazare will work independently from mobile devices which, according to Heath, is an attempt to avoid dependence upon the App Store and Google Play.[219] Hence, regulators should be aware that it may be some time before a truly open and interoperable metaverse is established as developing metaverse-related devices and selling them at a price that underbids the competition shows much more economic promise for companies in the short term.

Additionally, it is important to contextualise these economic incentives as they bleed into the other elements related to ethics, legality, and the user's experience. If left unaddressed, this may culminate in wider societal implications triggered by the prioritisation of profit generation above user-centricity. Regulators and private companies alike should aim to avoid a metaverse characterised by walled-garden platforms that will hinder the user's experience and the added value the metaverse can bring to human society. In addition to this, Meta's economic incentive to import its lucrative ads-based into the metaverse sparks genuine concerns of how personal data and the right to privacy will be protected in a Meta-led metaverse. Furthermore, many authors have warned that the metaverse may usher in a new age of XR-driven surveillance capitalism in which corporate power trumps human rights protection.[220] Hence, future regulation should focus on strengthening the enforceability of the UNGPs and curbing Meta's anti-competitive business practices to ensure that the company complies with global standards of data and consumer protection and to prevent further abuse of the human right to privacy.

Mandate the Prioritisation of UX/UI Design

Intricately linked to economic incentives is the element of user-centric design in the metaverse. User-centricity is relevant not only when designing products with consumer privacy and safety

[217] Alex Heath, 'Leaked Files Show Facebook Is in Crisis Mode over Losing Young People' The Verge (25 October 2021) <https://www.theverge.com/22743744/facebook-teen-usage-decline-frances-haugen-leaks> accessed 7 July 2022.
[218] Heath (n 57).
[219] ibid.
[220] Charamba (n 145).

in mind, but also when considering the overall added value of the metaverse. Lamentably, non-prioritisation of the user's experience has become a common feature of Web 2.0 technologies. Many companies, particularly in the health app space, push new products that are not fit for purpose and do not comply with relevant guidelines, but are designed for the primary purpose of gathering user data which is then sold to third parties. Any associated benefits of such technologies are considered as mere byproducts.[221] Regulators should aim to avoid the replication of this Web 2.0 issue in the metaverse where the potential for abuse of the consumer's privacy and safety will inevitably be heightened.

On a positive note, the Web 3.0 trends in favour of decentralisation and data sovereignty as well as recent calls for the recognition of the right to data ownership promise to guarantee user-centricity in the metaverse and should be reflected in forthcoming legislation.[222] By requiring companies to prioritise user-centric design principles, regulators would help to ensure that the powerful new technologies under development at Facebook Reality Labs are designed to advance human society in line with the true purpose of innovation. Therefore, future regulation should mandate that privacy by design, security, and safety by design principles are built into metaverse technology, which should be accompanied by an effective monitoring framework to audit regulatory compliance.[223]

Additionally, regulation needs to provide companies with clear guidelines on how user's rights should be communicated to them in the metaverse. This will prevent issues discussed in chapter two of this paper pertaining to the ambiguities left behind by the GDPR with regards to obtaining valid consent for biometric data processing in Web 2.0. Lastly, it is imperative that companies like Meta with a seminal role to play in the metaverse of the future align themselves with relevant industry codes of conduct that protect user rights. For example, the Oasis User Safety Standards spearheaded by Tiffany Xingyu Wang is a set of standards released in 2022 by the think tank OASIS Consortium in an effort to ingrain safety into our digital future, including the metaverse.[224] Companies may pledge to comply with these standards, use them to conduct internal self-assessments, and work towards earning a certification in 'Oasis Digital Sustainability in User Safety.' This includes establishing an independent advisory board to

[221] Quinn Grundy, 'A Review of the Quality and Impact of Mobile Health Apps' (2022) 43(1) Annual Review of Public Health 117, 122.
[222] Mack (n 180).
[223] Ann Cavoukian, 'Privacy by Design: The Definitive Workshop. A Foreword by Ann Cavoukian, Ph.D' (2010) 3 Identity in the Information Society 247.
[224] OASIS Consortium, *User safety standards for our digital future* (2021).

review decisions, making community guidelines easily accessible, and conducting audits on the effectiveness of content moderation tools, among other measures.[225] Similarly, Jessica Outlaw has developed the 'Seven Metaverse Privacy Principles' aimed at metaverse creators based on her research into the dark patterns associated with extensive data processing.[226] While these codes of conduct are rather idealistic and not legally binding, they can work in conjunction with effective regulation to build a more user-centric metaverse.

Rectify the Identified Legal Issues

The legal issues posed by Meta's new metaverse technologies have been well documented throughout this paper. However, this research has also revealed that lawmakers do not necessarily need to reinvent the wheel when it comes to its governance as potential remedies from existing areas of public and private law have also been discussed. Similarly, lawmakers can use the lessons learned from previous attempts to regulate the internet, social media, and video games to inform the legislative process. Overall, it is important that the necessary legislative reforms are accurately identified and promptly implemented in order to solve the issues that will be inherited from Web 2.0 and to cover the new threats posed by Web 3.0 technologies. This feat must be achieved in a timely manner to avoid replicating the current scenario of retrofitting reactionary legislation after major abuses of human rights have already occurred.

This paper has identified numerous legal challenges associated with the human rights implications of Meta's vision for the metaverse. First, the extensive collection and processing of biometric data poses major threats to information security and raises concerns about valid consent for data processing in the metaverse. Second, the inferences that can be made about a person's thoughts, interests, mood, and personality from such extensive biometric data collection may call for refinement of the legal definition for biometric data and an extension of the right to privacy in international and customary law to include mental privacy. This could be reinforced by the soft law of the UN in the form of a corporate responsibility to protect human rights in the digital realm. Third, the issue of either attributing a legal personality to Codec Avatars or establishing legal ownership over the personal data used to build them in accordance with property law was discussed as a means of mitigating digital harms caused by illegal avatar behaviour. Lastly, I posited the possibility of making reforms to laws surrounding

[225] ibid.
[226] Jessica Outlaw, 'Seven Metaverse Privacy Principles' *Medium* (11 March 2022) <https://jessica-outlaw.medium.com/7-metaverse-privacy-principles-1329dc321720> accessed 7 July 2022.

sexual harassment and assault in response to claims of sexual harassment in social virtual reality which will constitute a large part of Meta's metaverse.

These legal considerations are by no means extensive nor are the potential solutions considered fail-safe proposals. By contrast, I have identified the most pertinent legal issues associated with Meta's metaverse ambitions that are in need of prompt resolution in order to prevent major violations of global human rights norms. Future scholarship may address the broader legal concerns associated with the metaverse that fall outside the scope of this paper, such as ambiguities surrounding jurisdiction, intellectual property rights and NFTs, and anti-trust legislation.[227] This paper has also tackled the subject from a specifically European perspective by relying predominantly on Western conceptions of human rights, EU law, and the treaties of the Council of Europe. Therefore, there are a number of potential legal issues that this paper has left unaddressed that may be more relevant in less interventionist jurisdictions, such as the United States, where most big tech companies are also incorporated.

Consider the Broader Socio-Ethical Implications

Meta's metaverse ambitions also harbour several unintended socio-ethical consequences for today's society that derive from the three aforementioned elements. This paper has discussed numerous ethical quandaries, including the harms associated with immersive advertising and ineffective content moderation in the metaverse. However, perhaps the most prominent ethical consideration that regulators must be cognizant of is the potential for the metaverse to exacerbate existing discrimination and inequality. Technology is not impartial to the sexist, racist, or ableist tendencies of its creators. Sandra Wachter and Andrew McStay have already pointed out the discriminatory effects of affinity profiling and the biased algorithms employed by major social media companies.[228,229] The real-world consequences of such predatory algorithms hidden behind individualised social media feeds have already come to light by engendering radicalisation and division in many countries. For example, the January 6th insurrection at the US Capitol Building was facilitated by extremist Facebook groups and it was only after this event that Zuckerberg announced the company would no longer suggest political groups to users on Facebook.[230] In the context of the metaverse, the true extent of

[227] Wee and others (n 197).
[228] Wachter (n 132).
[229] McStay (n 128).
[230] Rys Farthing and Dhakshayini Sooriyakumaran, 'Why the Era of Big Tech Self-Regulation Must End' (2021) 92(4) AQ: Australian Quarterly 3, 7.

discrimination and its effects will be virtually invisible in a decentralised digital realm with no central governing structure. Therefore, it is crucial that future legislation protects users from algorithmic bias, as called for by the Neurorights Foundation.[231]

Similarly, Meta's hardware devices must be designed with inclusivity in mind. In 2020, MIT researcher Arwa Michelle Mboya brought the Oculus Go VR headset to Kenya to conduct a study on VR adoption. However, she found that every other time a participant attempted to use the headset, the strap broke as it was not designed to accommodate the texture and styling of Black hair.[232] Moreover, a 2020 study found that simulation sickness in virtual reality was more common in women than men because VR headsets are made to fit the interpupillary distance of the average male.[233] Additionally, in a 2021 study, Egliston and Carter highlighted the disabling effects of body tracking in VR which sees any deviances from the 'white, able-bodied, heterosexual, and male' body as abnormal and problematic.[234] This highlights the importance of diversity in research and development teams to ensure that these subconscious biases do not creep into the final product design. Ultimately, regulators must be aware that the metaverse has the potential to deepen the digital divide and become an incredibly unwelcome and unequal space for underrepresented groups in society.

The mental health of users is another socio-ethical issue associated with the metaverse that is addressed throughout this paper. Considering that Zuckerberg foresees individuals spending extended periods of time in the metaverse, greater transparency is required about the effects of long-term use and screen addiction, especially among young people. Similarly, photorealistic avatars have the potential to exacerbate body image issues among the population, as demonstrated by Jennifer Ogle.[235] This finding comes in the wake of revelations made by whistle-blower Frances Haugen which revealed that Meta is aware of the harmful effects its algorithms have on the mental health of teen girls but chooses to prioritize financial gains above ethical and moral interests.[236] Hence, future regulation should consider appropriate safety and

[231] Genser, Hermann and Yuste (n 149).
[232] Arwa Michelle Mboya, 'The Oculus Go Wasn't Designed for Black Hair' Medium (12 November 2020) <https://debugger.medium.com/the-oculus-go-a-hard-ware-problem-for-black-women-225d9b48d098> accessed 8 July 2022.
[233] Kay Stanney, Cali Fidopiastis and Linda Foster, 'Virtual Reality Is Sexist: But It Does Not Have to Be' (2020) 7(4) Frontiers in Robotics and AI 1.
[234] Egliston, and Carter (n 18).
[235] Park and Ogle (n 168).
[236] Ryan Mac and Cecilia Kang, 'Whistle-Blower Says Facebook "Chooses Profits Over Safety"' *The New York Times* (3 October 2021) <https://www.nytimes.com/2021/10/03/technology/whistle-blower-facebook-frances-haugen.html> accessed 15 June 2022.

protection features to be integrated into the metaverse, especially with regards to young children.

In short, the closer we edge to a fully-fledged metaverse, the more socio-ethical problems that will arise. It is important for regulators must keep abreast of these developments in order to understand the impact that effective regulation can have on mitigating the unintended negative consequences of new technologies. This will be particularly felt by underrepresented groups in society, such as women, children, and people of colour. It is hoped that with the aid of measured regulatory efforts the metaverse can bring true added value to all members of society and become an environment where human rights are protected and enjoyed.

Conclusion

In conclusion, this study set out primarily to explore how human rights will be impacted by a Meta-led metaverse. This paper, therefore, asserts that the right to privacy and freedom from discrimination are most at risk. The vast data collection efforts needed to build digital twin Codec Avatars as well as other advanced metaverse technologies poses the largest threat to data protection rights and the right to privacy by extension. Additionally, it appears that the inability to moderate avatar behaviour in immersive reality will adversely impact women and other under-represented groups, hindering their freedom from discrimination. The second research question asked: what are the legal loopholes that these human rights implications expose in existing legislation? In short, intensive biometric data collection calls for a public law response by requiring companies to employ principles of data minimisation and security. Similarly, greater clarification is needed in data protection law, such as the GDPR, around obtaining valid consent for biometric data collection in the metaverse. Heller's theory of biometric psychography was discussed in the context of adjusting the definition for biometric data, including a corporate responsibility to protect in the UNGPs, and extending the right to privacy to include mental privacy. In addition to this, the use of photorealistic Codec Avatars in extended reality environments suggests the impending need for a right to data ownership and/or legal personality to be attributed to avatars in the long term. Lastly, the issue of virtual sexual harassment perpetrated in the metaverse requires updates to be made to existing criminal law.

The third research question guided the analysis in final four which describes four key considerations for regulators to take into account in relation to metaverse governance. These key recommendations are to: (1) consider the economic incentives at play; (2) mandate the prioritisation of UX/UI design; (3) rectify the identified legal issues and (4) consider the broader socio-ethical implications when regulating for a human rights-compliant metaverse in the future. These four considerations are clearly defined yet highly interdependent. For example, user-centricity is impossible to achieve without creating an economic incentive to do so. Similarly, effective legal remedies will mitigate the adverse socio-ethical impacts of the metaverse. It is important to note that these recommendations are seen as a point of departure for metaverse governance and are open to further elaboration as we approach a fully coalesced metaverse in the coming years.

Additionally, the qualitative case-study approach taken by this research has allowed for a thorough investigation into Meta's new technologies and their broader context within Web 3.0 and the push for the metaverse. At the company's 2021 Connect Conference, CEO Mark Zuckerberg detailed a number of metaverse projects under development at Facebook Reality Labs, including state of the art AR glasses, VR headsets, BCI devices, and photorealistic digital twin avatars. These devices will be key to achieving realistic social presence in the metaverse and blurring the user's perception of the distinction between the real and the virtual worlds, in line with Meta's vision for the future. These technologies have the potential to render our digital interactions much more human by revolutionising the way we work, learn, and socialise. However, these expectations must be tempered by effective regulation that will allow the benefits of such technologies to be enjoyed by all.

Lastly, the major limitation associated with this study is the heavy reliance it places on less academic sources, such as newspaper articles, for the most up to data information on metaverse-related developments. In a similar vein, while this paper identifies some of the most pressing legal issues related to human rights in the metaverse, this list is not exhaustive. Notwithstanding these limitations, this study has certainly contributed to a growing body of work which aims to demystify the metaverse and its associated human rights implications. Thus, future research in this field can address the legal and ethical implications arising from issues such as the ownership of digital assets, environmental costs, and punishing crime in the metaverse. Moreover, this topic could also be addressed from the perspective of different corporations and jurisdictions for a broader understanding of the potential remedies available for solving virtual legal anomalies. It is only through further academic research into this topic that relevant laws and policies can be reformed in order to prevent further violations of fundamental human rights going forward.

Bibliography

Cases, EU legislation, and UN documents

Case C - 446/21 Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 20 July 2021 — Maximilian Schrems v Facebook Ireland Ltd [2021] OJ C 422/08.

Case C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband v. Planet49 GmbH [2019] ECR 801

Convention on the Elimination of All Forms of Discrimination Against Women (adopted 13 December 1979, entered into force 3 September 1981) 1249 UNTS 13 (CEDAW)

Court of Justice of the European Union Press Release No. 125/19, 'Storing cookies requires internet users' active consent' (1 October 2019) <https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-10/cp190125en.pdf> accessed 28 May 2022

Council of Europe, 128th session of the Committee of Ministers 'Convention 108+: Convention for the protection of individuals with regards to the processing of personal data' (18 May 2018)

Group of Experts on Action against Violence against Women and Domestic Violence 'GREVIO General Recommendation No. 1 on the Digital Dimension of Violence against Women' (adopted 20 October 2021)

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR)

OHCHR, 'Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework' (16 June 2011) UN Doc HR/PUB/11/104

Ordinanza ingiunzione nei confronti di Clearview AI [2022] Guarante per la Protezione dei Dati Personali 9751362

Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) [2020] COM/2020/767 final

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/32

Title 1.81.5. California Consumer Privacy Act of 2018 [1798.100 1798.199.100] ch 55, sec 3

UNCHR 'The Right to Privacy in the Digital Age - Report of the United Nations High Commissioner for Human Rights' (30 June 2014) UN Doc A/HRC/27/37

UN Broadband Commission for Digital Development Working Group on Broadband and Gender, 'Cyber Violence Against Women and Girls: A World-Wide Wake Up Call' (23 October 2015) <https://en.unesco.org/sites/default/files/genderreport2015final.pdf> accessed 12 May 2022

UN Committee on the Elimination of All Forms of Violence Against Women, 'General Recommendation No 35 on gender-based violence against women, updating general recommendation No. 19 (2017) UN Doc C/GC/35

UN Committee on the Elimination of Discrimination Against Women, 'General Recommendation No 19 of CEDAW on Violence Against Women (11th session, 1992), UN Doc HRI/Gen/1/Rev.6

Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR)

Volodina v Russia (no. 2) App no 40419/19 (ECtHR, 14 September 2021)

Books, Journal Articles, and Reports

Ahmed J and others, 'GDPR Compliant Consent Driven Data Protection in Online Social Networks: A Blockchain-Based Approach,' (2020) 3rd International Conference on Information and Computer Technologies (ICICT)

Amnesty International, 'Toxic Twitter - Triggers of Violence and Abuse Against Women on Twitter' <https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women-chapter-2/> accessed 12 May 2022

Amnesty International, 'Troll Patrol Findings: Using Crowdsourcing, Data Science & Machine Learning to Measure Violence and Abuse against Women on Twitter' <https://decoders.amnesty.org/projects/troll-patrol/findings> accessed 12 May 2022

Baxter P and S Jack, 'Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers' (2015) 13(4) The Qualitative Report 544 <https://nsuworks.nova.edu/tqr/vol13/iss4/2/> accessed 19 June 2022

Bhirangi R and others, 'ReSkin: versatile, replaceable, lasting tactile skins' (2021) 5th Conference on Robot Learning <https://reskin.dev/?fbclid=IwAR2G39gcfVuDpy1uru6qNds47N5QwWJtztSkgZUlrXJXSDJpYxKgyu2nvF0> accessed 22 May 2022

Blackwell L and others, 'Harassment in Social Virtual Reality: Challenges for Platform Governance' (2019) 3 Proceedings of the ACM on Human-Computer Interaction 1

Brenner SW, 'Fantasy Crime: The Role of Criminal Law in Virtual Worlds' (2008) 11(1) Vanderbilt Journal of Entertainment and Technology Law 1

Burke J, '>The Open Metaverse OS_' (January 2021) <https://outlierventures.io/wp-content/uploads/2021/08/OV-Metaverse-OS_V6.pdf> accessed 17 April 2022

Bye K, State of Privacy in XR & Neuro-Tech: Conceptual Frames' (4 June 2021) <https://www.youtube.com/watch?v=pIpD4-gYImU> accessed 6 May 2022

Cabañas JG and others, 'Does Facebook Use Sensitive Data for Advertising Purposes?' (2021) 64(1) Communications of the ACM 62

Cavoukian A, 'Privacy by Design: The Definitive Workshop. A Foreword by Ann Cavoukian, Ph.D' (2010) 3 Identity in the Information Society 247

Charamba K, 'Beyond the Corporate Responsibility to Respect in the Dawn of a Metaverse' (2022) University of Hong Kong Faculty of Law Research Paper No. 2022/14 1 <http://dx.doi.org/10.2139/ssrn.4043254> accessed 6 May 2022

Cheong BC, 'Avatars in the metaverse: potential legal issues and remedies' (2022) Int. Cybersecur. Law Rev. <https://doi.org/10.1365/s43439-022-00056-9> accessed 3 July 2022

De Vido S, 'The Istanbul Convention and Its Impact on EU Law and Policies' Ca' Foscari University of Venice (Trier, 20 November 2018)

Dionisio JDN, WG Burns III, and R Gilbert, '3D Virtual worlds and the metaverse: Current status and future possibilities' (2013) 45(3) ACM Computing Surveys 1 <http://dx.doi.org/10.1145/2480741.2480751> accessed 22 June 2022

Dutra da Cunha R, FW Neiva and RL de Souza da Silva, 'Virtual Reality as a Support Tool for the Treatment of People with Intellectual and Multiple Disabilities: A Systematic Literature Review' (2018) 25(1) Revista de Informática Teórica e Aplicada 67

Egliston B and M Carter, 'Critical questions for Facebook's virtual reality: data, power and the metaverse' (2021) 10(4) Internet Policy Review <https://doi.org/10.14763/2021.4.1610> accessed 18 April 2022

European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (4 May 2020) <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf > accessed 28 May 2022

eSafety Commissioner, 'Immersive Technologies – Position Statement' (10 December 202) <https://www.esafety.gov.au/industry/tech-trends-and-challenges/immersive-tech> accessed 15 May 2022

Far S and A Rad, 'Applying Digital Twins in Metaverse: User Interface, Security and Privacy Challenges' (2022) 2(1) Journal of Metaverse 8

Farthing R and D Sooriyakumaran, 'Why the Era of Big Tech Self-Regulation Must End' (2021) 92(4) AQ: Australian Quarterly 3

Freeman G and others, 'My Body, My Avatar: How People Perceive Their Avatars in Social Virtual Reality' (2020) Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems <https://dl.acm.org/doi/10.1145/3334480.3382923> accessed 14 May 2022

Garon J, 'Legal Implications of a Ubiquitous Metaverse and a Web3 Future' (2022) <http://dx.doi.org/10.2139/ssrn.4002551> accessed July 14 2022

Genser J, S Herrmann, and R Yuste, *International Human Rights Protection Gaps in the Age of Neurotechnology* (NeuroRights Foundation 2022)

Grundy Q, 'A Review of the Quality and Impact of Mobile Health Apps' (2022) 43(1) Annual Review of Public Health 117

Hartzog W, 'BIPA: The Most Important Biometric Privacy Law in the US?' in Amba Kak (ed) *Regulating Biometrics: Global Approaches and Urgent Questions* (AI Now Institute 2020)

Heller B, 'Reimagining Reality: Human Rights and Immersive Technology' (Carr Center Discussion Paper Series 2020)

Heller B and A Bar-Zeev, 'The Problems with Immersive Advertising: In AR/VR, Nobody Knows You Are an Ad' (2021) 1(1) Journal of Online Trust and Safety 1 <https://tsjournal.org/index.php/jots/article/view/21> accessed 7 May 2022

Hodson J and P Livingstone, 'View of Playing in Drag: A Study on Gender In Virtual and Non-Virtual Gaming' (2017) 10(16) The Journal of the Canadian Game Studies Association 109 <https://journals.sfu.ca/loading/index.php/loading/article/view/182/209https://journals.sfu.ca/loading/index.php/loading/article/view/182> accessed 14 May 2022

International Association of Privacy Professionals, 'LIVE IAPP Summit 2022 General Session with Tim Cook, Zahra Mosawi, Didier Reynders and Trevor Hughes' (12 April 2022) <https://youtu.be/Dq0fcmmzfog?t=11> accessed 28 May 2022

Johnston MP, 'Secondary Data Analysis: A Method of which the Time Has Come' (May 2017) 3(3) Qualitative and Quantitative Methods in Libraries 619 <http://www.qqml-journal.net/index.php/qqml/article/view/169> accessed 19 June 2022

Kröger JL, OHM Lutz and F Müller, 'What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking' in Michael Friedewald, Melek Önen, Eva Lievens, Stephan Krenn and Samuel Fricker (eds), *Privacy and Identity Management. Data for Better Living: AI and Privacy* (Springer 2020) <https://link.springer.com/chapter/10.1007/978-3-030-42504-3_15> accessed 26 June 2022

Kröger JL, OHM Lutz and P Raschke, 'Privacy Implications of Voice and Speech Analysis – Information Disclosure by Inference' in Michael Friedewald, Melek Önen, Eva Lievens, Stephan Krenn and Samuel Fricker (eds), *Privacy and Identity Management. Data for Better Living: AI and Privacy*, (Springer 2020) <http://link.springer.com/10.1007/978-3-030-42504-3_16> accessed 26 June 2022

Lau PL, 'An Ecosystem of Interconnectedness: Prioritising Key Legal Concerns in the Metaverse' *The World Financial Review* (25 May 2022) <https://worldfinancialreview.com/an-ecosystem-of-interconnectedness-prioritising-key-legal-concerns-in-the-metaverse/> accessed 3 July 2022

Lemley M and E Volokh, 'Law, Virtual Reality, and Augmented Reality' (2018) 166(5) U. PA. L. REV 1051

Makransky G and RE Mayer, 'Benefits of Taking a Virtual Field Trip in Immersive Virtual Reality: Evidence for the Immersion Principle in Multimedia Learning' (2022) Educ Psychol Rev <https://doi.org/10.1007/s10648-022-09675-4> accessed 25 June 2022

Mansourian Y, 'Exploratory Nature of, and Uncertainty Tolerance in, Qualitative Research' (2008) 109 New Library World 273

McStay A, ‘Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy’ (2020) 7 Big Data & Society 1

Meta, ‘The Metaverse and How We’ll Build It Together -- Connect 2021’ (28 October 2021) <https://youtu.be/Uvufun6xer8?t=1> accessed 27 March 2022

Meta Platforms, Inc., ‘Meta Reports Fourth Quarter and Full Year 2021 Results’ (2 February 2022) <https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx> accessed 19 June 2022

Meta Platforms, Inc., Notice of Annual Meeting & Proxy Statement (2022) <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/22a38320-0a0a-4f62-935d-41ab580273de.pdf> accessed 21 May 2022

Metaverse Standards Forum, ‘Leading Standards Organizations and Companies Unite to Drive Open Metaverse Interoperability’ (12 May 2022) <https://metaverse-standards.org/news/press-releases/leading-standards-organizations-and-companies-unite-to-drive-open-metaverse-interoperability/> accessed 21 June 2022

Nevelsteen K, 'Metaverse Interoperability Keynote (with Slides and Annotation) AIBC UAE 2022' (5 May 2022) <https://www.youtube.com/watch?v=3dxrAvjaqf8> accessed 22 May 2022

OASIS Consortium, *User safety standards for our digital future* (2021)

Park J and JP Ogle, ‘How virtual avatar experience interplays with self-concepts: the use of anthropometric 3D body models in the visual stimulation process’ (2021) 8(28) Fash Text 1 <https://doi.org/10.1186/s40691-021-00257-6> accessed 14 May 2022

Peck TC and others, ‘Putting Yourself in the Skin of a Black Avatar Reduces Implicit Racial Bias’ (2013) 22(3) Consciousness and Cognition 779

Rodriguez K and K Opsahl, ‘Augmented Reality Must Have Augmented Privacy’ *Electronic Frontier Foundation* (16 October 2020) <https://www.eff.org/deeplinks/2020/10/augmented-reality-must-have-augmented-privacy> accessed 25 June 2022

Rodriguez K and others, ‘Virtual Worlds, Real People: Human Rights in the Metaverse’ *Electronic Frontier Foundation, Access Now* (9 December 2021) <https://www.eff.org/deeplinks/2021/12/virtual-worlds-real-people-human-rights-metaverse> accessed 18 June 2022

Stanney K, C Fidopiastis and L Foster, ‘Virtual Reality Is Sexist: But It Does Not Have to Be’ (2020) 7(4) Frontiers in Robotics and AI 1

Stephenson N, *Snow Crash* (Penguin 1992)

The Berkman Klein Center for Internet & Society, ‘William Fisher, CopyrightX: Lecture 2.1, Fairness and Personality Theories: Introduction’ (16 January 2015) <https://www.youtube.com/watch?v=nKyWusznRgQ> accessed 14 May 2022

Thomason J, 'MetaHealth - How will the Metaverse Change Health Care?' (2021) 1(1) Journal of Metaverse 13 <https://dergipark.org.tr/en/download/article-file/2167692> accessed 25 June 2022

Wachter S, 'Affinity Profiling and Discrimination by Association in Online Behavioural Advertising' (2020) 35(2) Berkeley Technology Law Journal 1 (forthcoming)

Warren S and L Brandeis, 'The Right to Privacy' (1890) 4(5) Harvard Law Review <https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html> accessed 26 April 2022

XRSI, 'The Child Safety Initiative' <https://xrsi.org/programs/child-safety> accessed 3 July 2022

Yee N and J Bailenson, 'The Proteus Effect: The Effect of Transformed Self-Representation on Behavior' (2007) 33 Human Communication Research 271

Zuboff S, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019)

Websites and Newspaper Articles

Alspach K, 'Why the Fate of the Metaverse Could Hang on Its Security' *VentureBeat* (26 January 2022) <https://venturebeat.com/2022/01/26/why-the-fate-of-the-metaverse-could-hang-on-its-security/> accessed 28 May 2022

'Audio- and Gaze-Driven Facial Animation of Codec Avatars' *Meta Research* (17 December 2021) <https://research.facebook.com/videos/audio-and-gaze-driven-facial-animation-of-codec-avatars/> accessed 19 April 2022

Ball M, 'Hardware and the Metaverse' *MatthewBall.vc* (29 June 2021) <https://www.matthewball.vc/all/hardwaremetaverse> accessed 21 May 2022

Ball M, 'The Metaverse: What It Is, Where to Find It, and Who Will Build It' *MatthewBall.vc* (13 January 2020) <https://www.matthewball.vc/all/themetaverse> accessed 26 March 2022

Barbaro M, 'Microsoft and the Metaverse' *The New York Times* (20 January 2022) 06.30 <https://www.nytimes.com/2022/01/20/podcasts/the-daily/metaverse-microsoft-activision-blizzard.html> accessed 19 April 2022

Bareckas K, 'Would You Join the Metaverse?' *NordVPN* (25 January 2022) <https://nordvpn.com/blog/metaverse-survey/> accessed 28 May 2022

Bar-Zeev A, 'For XR, the Eyes Are the Prize' *Medium* (17 November 2020) <https://avibarzeev.medium.com/for-xr-the-eyes-are-the-prize-25d43a533f2a> accessed 30 April 2022

Basu T, 'The Metaverse Is the next Venue for Body Dysmorphia Online' *MIT Technology Review* (16 November 2021)

<https://www.technologyreview.com/2021/11/16/1040174/facebook-metaverse-body-dysmorphia/> accessed 14 May 2022

Belamire J, 'My First Virtual Reality Groping' *Athena Talks* (22 October 2016) <https://medium.com/athena-talks/my-first-virtual-reality-sexual-assault-2330410b62ee> accessed 15 May 2022

Bell C, 'The Metaverse Is Coming. Here Are the Cornerstones for Securing It.' *The Official Microsoft Blog* (28 March 2022) <https://blogs.microsoft.com/blog/2022/03/28/the-metaverse-is-coming-here-are-the-cornerstones-for-securing-it/> accessed 21 May 2022

Brandom R, 'Even If You're Not Signed up, Facebook Has a Shadow Profile for You' *The Verge* (11 April 2018) <https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy> accessed 23 April 2022

Browne R, 'Sony and the Lego Family Bet Big on the "metaverse" with $2 Billion Investment in Epic Games' *CNBC* (11 April 2022) <https://www.cnbc.com/2022/04/11/sony-and-lego-family-invest-2-billion-in-fortnite-creator-epic-games.html> accessed 11 April 2022

Center for Countering Digital Hate, 'Facebook's Metaverse Is Unsafe' *CCDH* (30 December 2021) <https://www.counterhate.com/metaverse> accessed 15 May 2022

Chakraborty K, 'What Is Web 1.0? - Definition from Techopedia' *Techopedia.com* (29 June 2021) <http://www.techopedia.com/definition/27960/web-10> accessed 22 May 2022

Clarke L, 'Can We Create a Moral Metaverse?' *The Guardian* (14 May 2022) <https://www.theguardian.com/technology/2022/may/14/can-we-create-a-moral-metaverse> accessed 3 July 2022

Cortese M, 'Designing Safer Social VR' *Medium* (19 November 2019) <https://immerse.news/designing-safer-social-vr-76f99f0be82e> accessed 16 May 2022

European Parliament, Digital Services: landmark rules adopted for a safer, open online environment' (5 July 2022) <https://www.europarl.europa.eu/news/en/press-room/20220701IPR34364/digital-services-landmark-rules-adopted-for-a-safer-open-online-environment> accessed 7 July 2022

Davies R, '"Conditioning an Entire Society": The Rise of Biometric Data Technology' *The Guardian* (26 October 2021) <https://www.theguardian.com/technology/2021/oct/26/conditioning-an-entire-society-the-rise-of-biometric-data-technology> accessed 26 June 2022

Dixon C [@cdixon], 'Web1: Read Web2: Read, Write Web3: Read, Write, Own' *Twitter* (8 February 2022) <https://twitter.com/cdixon/status/1490866307599794180> accessed 22 May 2022

'Extended Reality (XR)' *Electronic Frontier Foundation* <https://www.eff.org/issues/xr> accessed 21 April 2022

‘Facebook is Building the Future of Connection with Lifelike Avatars’ *Tech at Meta* (13 March 2019) <https://tech.fb.com/ar-vr/2019/03/codec-avatars-facebook-reality-labs/> accessed 23 May 2022

Frier S and D Bass, ‘Microsoft Makes a $69 Billion Down Payment on the Metaverse’ *Bloomberg* (19 January 2022) <https://www.bloomberg.com/news/articles/2022-01-19/microsoft-msft-activision-blizzard-atvi-deal-shows-big-tech-metaverse-push> accessed 16 April 2022

Gent E, ‘Q&A: Why the Metaverse Needs to Be Open’ *IEEE Spectrum* (18 August 2021) <https://spectrum.ieee.org/open-metaverse> accessed 19 April 2022

Hackl C, ‘Defining The Metaverse Today’ *Forbes* (2 May 2021) <https://www.forbes.com/sites/cathyhackl/2021/05/02/defining-the-metaverse-today/> accessed 20 June 2022.

Harris T, ‘The Muddled Metaverse - A Case against NFT Interoperability in Videogames.’ *LinkedIn* (1 January 2022) <https://www.linkedin.com/pulse/muddled-metaverse-case-against-nft-interoperability-todd-harris/> accessed 21 June 2022

Hayden S, ‘Meta to Merge “Venues” Event Space into “Horizon Worlds” Social VR Platform’ *Road to VR* (9 May 2022) <https://www.roadtovr.com/meta-venues-events-horizon-worlds-quest-2/> accessed 15 May 2022

Hayward A, ‘“No Company Can Own” the Metaverse, Says Epic Games CEO’ *Decrypt* (17 November 2021) <https://decrypt.co/86323/no-company-can-own-metaverse-epic-games-ceo-tim-sweeney> accessed 22 May 2022

Heath A, ‘Facebook Debuts Ray-Ban Stories, Smart Glasses That Record Video’ *The Verge* (9 September 2021) <https://www.theverge.com/2021/9/9/22662809/facebook-ray-ban-stories-camera-smart-glasses-hands-on> accessed 22 May 2022

Heath A, ‘Leaked Files Show Facebook Is in Crisis Mode over Losing Young People’ *The Verge* (25 October 2021) <https://www.theverge.com/22743744/facebook-teen-usage-decline-frances-haugen-leaks> accessed 7 July 2022

Heath A, ‘Mark Zuckerberg on Why Facebook Is Rebranding to Meta’ *The Verge* (28 October 2021) <https://www.theverge.com/22749919/mark-zuckerberg-facebook-meta-company-rebrand> accessed 18 June 2022

Heath A, ‘Mark Zuckerberg’s Augmented Reality’ *The Verge* (13 April 2022) <https://www.theverge.com/23022611/meta-facebook-nazare-ar-glasses-roadmap-2024> accessed 19 April 2022

Heath A, ‘Meta’s Social VR Platform Horizon Hits 300,000 Users’ *The Verge* (17 February 2022) <https://www.theverge.com/2022/2/17/22939297/meta-social-vr-platform-horizon-300000-users> accessed 11 June 2022

Hoium T, 'Oculus Devices Sold Out in a Positive Sign for Virtual Reality' *The Motley Fool* (27 December 2019) <https://www.fool.com/investing/2019/12/27/oculus-devices-sold-out-in-positive-sign-for-virtu.aspx> accessed 11 June 2022

Hutt R, 'What Are Your Digital Rights?' *World Economic Forum* (13 November 2015) <https://www.weforum.org/agenda/2015/11/what-are-your-digital-rights-explainer/> accessed 22 May 2022

'Inside Reality Labs Research: Meet the Team That's Working to Bring Touch to the Digital World' *Tech at Meta* (16 November 2021) <https://tech.fb.com/ar-vr/2021/11/inside-reality-labs-meet-the-team-thats-bringing-touch-to-the-digital-world/> accessed 22 May 2022

'Inside Facebook Reality Labs: Wrist-Based Interaction for the next Computing Platform' *Tech at Meta* (18 March 2021) <https://tech.fb.com/ar-vr/2021/03/inside-facebook-reality-labs-wrist-based-interaction-for-the-next-computing-platform/> accessed 22 May 2022

Kastrenakes J, 'Facebook Is Spending at Least $10 Billion This Year on Its Metaverse Division' *The Verge* (25 October 2021) <https://www.theverge.com/2021/10/25/22745381/facebook-reality-labs-10-billion-metaverse> accessed 18 April 2022

Khitrov A, 'What Will It Take to Stop Fraud in the Metaverse?' *Information Age* (29 March 2022) <https://www.information-age.com/what-will-it-take-to-stop-fraud-in-metaverse-123499073/> accessed 28 May 2022

Kovach S, 'How the Metaverse Won Christmas' *CNBC* (27 December 2021) <https://www.cnbc.com/2021/12/27/metas-oculus-virtual-reality-headsets-were-a-popular-holiday-gift.html> accessed 11 June 2022

Lorenz T, 'Virtual Reality Is Full of Assholes Who Sexually Harass Me. Here's Why I Keep Going Back' *Mic* (26 May 2016) <https://www.mic.com/articles/144470/sexual-harassment-in-virtual-reality> accessed 15 May 2022

Mac R and C Kang, 'Whistle-Blower Says Facebook "Chooses Profits Over Safety"' *The New York Times* (3 October 2021) <https://www.nytimes.com/2021/10/03/technology/whistle-blower-facebook-frances-haugen.html> accessed 15 June 2022

Mac R, 'Facebook Is Considering Facial Recognition For Its Upcoming Smart Glasses' *BuzzFeed News* (25 February 2021) <https://www.buzzfeednews.com/article/ryanmac/facebook-considers-facial-recognition-smart-glasses> accessed 9 June 2022

Mack OV, 'Who Owns Your Digital Twin? Not You—and Here's Why That's a Massive Problem | Opinion' *Newsweek* (1 August 2019) <https://www.newsweek.com/who-owns-your-digital-twin-not-you-heres-why-thats-massive-problem-opinion-1451991> accessed 3 July 2022

Mboya AM, 'The Oculus Go Wasn't Designed for Black Hair' *Medium* (12 November 2020) <https://debugger.medium.com/the-oculus-go-a-hard-ware-problem-for-black-women-225d9b48d098> accessed 8 July 2022

Merchant B, 'The Metaverse Has Always Been a Dystopian Idea' *Vice* (30 July 2021). <https://www.vice.com/en/article/v7eqbb/the-metaverse-has-always-been-a-dystopia> accessed 21 May 2022

Meta, 'Introducing Project Aria' <https://about.facebook.com/realitylabs/projectaria/> accessed 9 June 2022

Meta Quest, 'Codec Avatars' (25 September 2019) <https://www.youtube.com/watch?v=Rqj956KgvRU> accessed 2 April 2022

Meta Quest, 'Full-Body Codec Avatars' (25 September 2019) <https://www.youtube.com/watch?v=_ZkG4iB_exU> accessed 23 May 2022

Meta Quest, 'Project Cambria Preview - Mixed Reality with Presence Platform' (12 May 2022) <https://www.youtube.com/watch?v=tgJ7m0Phd64> accessed 22 May 2022

'Metaverse Is Already Limiting Virtual Sexual Assault' *Verdict* (11 February 2022) <https://www.verdict.co.uk/metaverse-meta-sexual-assault/> accessed 16 May 2022

Mijatović D, 'No Space for Violence against Women and Girls in the Digital World' (*Council of Europe Portal*, 15 March 2022) <https://www.coe.int/en/web/commissioner/blog/-/asset_publisher/xZ32OPEoxOkq/content/no-space-for-violence-against-women-and-girls-in-the-digital-world> accessed 12 May 2022

Milmo D, 'Rohingya Sue Facebook for £150bn over Myanmar Genocide' *The Guardian* (6 December 2021) <https://www.theguardian.com/technology/2021/dec/06/rohingya-sue-facebook-myanmar-genocide-us-uk-legal-action-social-media-violence> accessed 21 May 2022

Murphy H, '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 27 March 2022

Murphy H, 'How Will Facebook Keep Its Metaverse Safe for Users?' *Financial Times* (12 November 2021) <https://www.ft.com/content/d72145b7-5e44-446a-819c-51d67c5471cf> accessed June 11 2022

Newton C, 'Mark Zuckerberg Is Betting Facebook's Future on the Metaverse' *The Verge* (22 July 2021) <https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview> accessed 26 March 2022

Norton Rose Fulbright 'The Metaverse: The Evolution of a Universal Digital Platform' (July 2021) <https://www.nortonrosefulbright.com/en/knowledge/publications/5cd471a1/the-metaverse-the-evolution-of-a-universal-digital-platform> accessed 5 May 2022

O'Regan SV, 'Meta Scales Back AR Glasses Plan Amid Reality Labs Shakeup' *The Information* (9 June 2022) <https://www.theinformation.com/articles/meta-scales-back-ar-glasses-plan-amid-reality-labs-shakeup> accessed 22 June 2022

Oremus W, 'Kids Are Flocking to Facebook's "Metaverse." Experts Worry Predators Will Follow.' *Washington Post* (7 February 2022) <https://www.washingtonpost.com/technology/2022/02/07/facebook-metaverse-horizon-worlds-kids-safety/> accessed 6 July 2022

Outlaw J, 'Seven Metaverse Privacy Principles' *Medium* (11 March 2022) <https://jessica-outlaw.medium.com/7-metaverse-privacy-principles-1329dc321720> accessed 7 July 2022

Outlaw J, 'Virtual Harassment: The Social Experience of 600+ Regular Virtual Reality (VR) Users' *Medium* (5 April 2018) <https://virtualrealitypop.com/virtual-harassment-the-social-experience-of-600-regular-virtual-reality-vr-users-23b1b4ef884e> accessed 15 May 2022

Perarnaud C, 'Privacy and Data Protection' *DW Observatory* <https://dig.watch/topics/privacy-and-data-protection> accessed 27 April 2022

Peters J, 'Meta Is Working on a Web Version of Its Horizon Worlds Metaverse Platform' *The Verge* (14 April 2022) <https://www.theverge.com/2022/4/14/23025899/meta-horizon-worlds-web-version-metaverse-platform> accessed 22 June 2022

Petter O, 'Why Is No One Taking Sexual Harassment In The Metaverse Seriously?' *British Vogue* (20 March 2022) <https://www.vogue.co.uk/arts-and-lifestyle/article/sexual-assault-in-the-metaverse> accessed 15 May 2022

Priestley T, 'Digital Twins, IOT and the Metaverse' *Medium* (5 August 2021) <https://medium.com/@theo/digital-twins-iot-and-the-metaverse-b4efbfc01112> accessed 22 April 2022

Purdy M, 'How the Metaverse Could Change Work' *Harvard Business Review* (5 April 2022) <https://hbr.org/2022/04/how-the-metaverse-could-change-work> accessed 25 June 2022

Reach3 Insights, 'Reach3 Insights' New Research Reveals 59% of Women Surveyed Use a Non-Gendered/Male Identity to Avoid Harassment While Gaming' (19 May 2021) <https://www.reach3insights.com/women-gaming-study> accessed 16 May 2022

Reuters, 'Austrian Activist Schrems' Facebook Complaint Referred to EU Court' (20 July 2021) <https://www.reuters.com/technology/austrian-activist-schrems-facebook-complaint-referred-eu-court-2021-07-20/> accessed 2 May 2022

RightsCon 2022, 'Every breath you take, every move you make: neurotechnology, XR, and the metaverse of surveillance' (6 June 2022) <https://rightscon.summit.tc/t/2022/events/every-breath-you-take-every-move-you-make-neurotechnology-xr-and-the-metaverse-of-surveillance-muemfgK7L82gzPRc7bPzGF> accessed 6 June 2022

Sun J, 'Why the Future of the Metaverse Can Only Be Decentralized' *VentureBeat* (5 March 2022) <https://venturebeat.com/2022/03/05/why-the-future-of-the-metaverse-can-only-be-decentralized/> accessed 22 May 2022

Surfshark, 'Apps That Track You and Their Alternatives' <https://surfshark.com/apps-that-track-you> accessed 25 June 2022

Takahashi D, 'The Ethics of the Metaverse' *VentureBeat* (27 January 2022) <https://venturebeat.com/2022/01/26/the-ethics-of-the-metaverse-2/> accessed 22 May 2022

'The Facebook Papers: What Do They Mean from a Human Rights Perspective?' *Amnesty International* (4 November 2021) <https://www.amnesty.org/en/latest/campaigns/2021/11/the-facebook-papers-what-do-they-mean-from-a-human-rights-perspective/> accessed 21 May 2022

Tunggal AT, 'The 63 Biggest Data Breaches (Updated for February 2022)' *UpGuard* (26 June 2022) <https://www.upguard.com/blog/biggest-data-breaches> accessed 30 April 2022

'Undercover Journalist Witnesses Abuse in Metaverse' *BBC News* (23 February 2022) <https://www.bbc.com/news/av/uk-60466557> accessed 11 June 2022

Vescent H, 'The Metaverse: A Missed Opportunity for Data Ownership and Privacy?' *Biometric Update* (21 January 2022) <https://www.biometricupdate.com/202201/the-metaverse-a-missed-opportunity-for-data-ownership-and-privacy> accessed 3 July 2022

Villas-Boas A, 'Scientists Looked at How Ugly Avatars Are Treated Compared to Hot Ones and Found an Unfortunate Truth' *Business Insider* (7 May 2015)

<https://www.businessinsider.com/how-good-your-avatar-looks-has-a-negative-impact-2015-5> accessed 14 May 2022

'Web3, the Metaverse, and the Future of the Internet' *Verdict* (17 March 2022) <https://www.verdict.co.uk/web3-metaverse-internet/> accessed 22 April 2022

Wee R, F Ismail and K Chan, 'The Metaverse and Its Legal Issues' *Richard Wee Chambers* (18 February 2022) <https://www.richardweechambers.com/the-metaverse-and-its-legal-issues/> accessed 1 June 2022

'What Is Web 2.0? - Definition from Techopedia' *Techopedia.com* (30 April 2020) <http://www.techopedia.com/definition/4922/web-20> accessed 22 June 2022