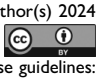
Article

Journal of Strategic Contracting and Negotiation
JSCAN

Disrupting MMORPGs gaming: Exploring and renegotiating end-user license agreements in the Metaverse

Journal of Strategic Contracting and Negotiation
1-23



DOI: 10.1177/20555636241246188
journals.sagepub.com/home/jsc


Pin Lean Lau
Brunel Law School, Brunel University London, Kingston Lane, UK

Abstract

This paper explores key legal issues surrounding gaming platforms that provide/host Massive Multiplayer Online Role-Playing Games. Since we are entering the next epoch of the Internet, Web3.0 – and the emergence of Metaverses that operate within this space, this paper conducts an inquiry into the key facets of end-user license agreements (EULAs) used in the platforms that may likely need to be renegotiated. Firstly, how do we reconcile the legal regulatory status of gaming platforms in a decentralized Web3.0 Metaverse? Secondly, how can the rights of end users of gaming platforms be protected vis-à-vis the EULAs in this space? And thirdly, what specific aspects in existing EULAs are likely needed to be renegotiated in light of a decentralized Web3.0 Metaverse? This paper will utilize a case study using the EULAs of Blizzard Entertainment Inc. and provide a possible reformulation of specific terms and conditions of EULAs.

Keywords

Artificial intelligence, metaverse, decentralized society, Web3.0, internet, gaming, MMORPG, EULAs

Introduction

Massive Multiplayer Online Role-Playing Games (MMORPGs), the epitome of online and virtual gaming platforms, possess an awe-inspiring allure that has captivated the masses. Their unique appeal lies not only in the immersive experiences they offer but in their remarkable capacity to forge the growth of communities, both online and offline, and transcend boundaries. The undeniable appeal of MMORPGs stems from their enthralling narratives, vast open worlds, intricate gameplay

Corresponding author:
Pin Lean Lau, Brunel Law School, Brunel University London, Kingston Lane, UB8 3PH, UK.
Email: pinlean.lau@brunel.ac.uk

mechanics and fantastical depictions of characters and worlds beyond ours – all capable of entangling players in an infinite tapestry of adventure, excitement and camaraderie. The popularity of MMORPGs is almost boundless, spread across demographics and cultures, resonating with an almost feverish fervour in collective consciousness of its players. As these immersive virtual realms continue to flourish, they are poised to disrupt various segments of the market industry, reshaping entertainment, social interactions, shopping and even business and commerce. The impact of MMORPGs is anticipated to be magnified within the Metaverse, a realm where digital experiences transcend reality, further blurring the lines between the virtual and the tangible. Within this grand tapestry of the Metaverse, the meteoric rise of MMORPGs is likely to continue to disrupt, altering the way we perceive, engage and ultimately exist within the boundless frontiers of the digital realm.

Whilst this may undoubtedly be pleasing to players of MMORPGs, it is interesting to consider how the conception of Web3.0, as a new version of the internet that prioritizes openness, decentralization (through blockchain technologies) and the return of 'power' into the hands of the community *vis-à-vis* collective decision-making mechanisms,[1] may impact MMORPGs gaming platforms.

Artificial intelligence and machine learning, having reached adequate technological maturity levels at this juncture, are in optimum position to synergize user interactions with the Internet, with algorithms tirelessly operating to analyze and extrapolate user-generated data.[2] Web3.0 therefore is likely to transform the way in which we use the Internet, with early signs of this development reflected in emergence of Metaverses, cryptocurrencies and non-fungible tokens (NFTs), amongst others.[3] Bearing in mind that the key concept of Web3.0 is a Decentralized Society (DeSoc), in the manner envisaged by, amongst others, the co-founder of Ethereum, Vitalik Buterin,[4] this paper is interested in responses of the online and/or virtual gaming industry, which is expected to be worth a whopping US$470 billion by 2030, and where the 'Metaverse and virtual reality will be a driving force of growth…'.[5]

This paper attempts to address the following questions: firstly, how do we (and can we) reconcile the legal regulatory status of gaming platforms in a decentralized Web3.0 Metaverse? Secondly, can the rights of end users of gaming platforms be protected *vis-à-vis* the end-user license agreements (EULAs) in this renewed space? And thirdly, what specific aspects in EULAs are likely needed to be renegotiated and/or reformulated in light of a decentralized Web3.0 Metaverse? For the purposes of the latter, the study in this paper will utilize a case study using the EULAs of Blizzard Entertainment Inc., arguably one of the most popular gaming platforms in the world (creators of World of Warcraft, Starcraft, Diablo and Overwatch), and provide a possible reinterpretation and renegotiation of specific terms and conditions in the EULAs. (For avoidance of doubt, the terminology 'gaming' referred to in this paper excludes all forms of gaming that relate to gambling, online

1. Peter Cooper, 'WEB 3.0 Impact on the Business and Legal Issues', Fintech Harbor Consulting, 3 October 2022, https://www.fintecharbor.com/web-3-0-impact-on-the-business-and-legal-issues/.

2. Polkadot.ERI, 'One Article to Understand The Past, Present, and Future of Web 3.0', *Polkadot Network* (blog), 7 December 2021, https://medium.com/polkadot-network/one-article-to-understand-the-past-present-and-future-of-web-3-0-5433962b7c3e.

3. Lau, 'The Murky Waters of the Metaverse', 76–83.

4. Weyl, Ohlhaver, and Buterin, 'Decentralized Society'.

5. Kurt Robson, 'Gaming Industry to Be Worth $470bn by 2030 despite Setbacks, Experts Predict', *Verdict* (blog), 3 April 2023, https://www.verdict.co.uk/gaming-industry-to-be-worth-470bn-by-2030-despite-setbacks-experts-predict/.

or offline or in arcades, adult gaming centers, betting shops, book makers, casinos and bingo venues).

Legal and regulatory status of MMORPG gaming platforms

In our contemporary technological epoch, the regulation of the Internet is a complex and multifaceted endeavour. Governments and international organizations often grapple between the need to foster digital innovations, whilst ensuring the protection of fundamental rights of users. Depending on jurisdiction, MMORPG gaming platforms, as one example of a highly successful Internet undertaking, are subject to evolving legal frameworks that are highly influenced by technological realities. Some key issues, such as data privacy, data protection, cybersecurity, content moderation and digital market competition, amongst others, will continue to be enduring determinants in the framework of regulation. The dynamic nature of the Internet as a continually emerging technology in our Anthropocene will often challenge traditional regulatory models, highlighting the accentuation for adaptability and agile approaches. Striving to harmonize global Internet standards whilst respecting cultural nuances, regulating the Internet means we must navigate a labyrinth of Gordian knots at each significant turn before we may ultimately shape a digital landscape that defines our interconnected worlds in responsible ways.

Showcasing the marvels of novel and emerging technologies forms the foundational cornerstone for initiating a dialogue concerning the Internet's regulation. A notable reference in this regards is Lawrence Lessig's *opus memorabile maximum*, The Code[6] elucidates the role of a prominent regulator in the realm of cyberspace governance. This imperative for 'regulability'[7] arises from the realization that the trajectory towards a technologically augmented state introduces a fresh peril of comprehensive control.[8] This concern, arguably, prompted the convening of a pivotal interdisciplinary conference in London in 2007, themed Regulating Technologies.[9] Despite prevailing apprehensions within the technological discourse, prophesying an Orwellian future, this paper contends that our focus should instead be meticulously attuned to the current implications of these technologies, that is, the Internet, in the present moment: such present moment being the entrance into Web3.0 and the Metaverse. The following sub-sections attempt to answer the first question posed in this paper: how do we (and can we) reconcile the legal regulatory status of gaming platforms in a decentralized Web3.0 Metaverse?

Governing MMORPGs on the internet

Taking the subject of this paper's discussion, the legal and regulatory status of MMORPGs in online and virtual gaming platforms remains a dynamic landscape, subject to a mosaic of national and international laws in its present iteration. Primarily categorized as digital services, MMORPGs often traverse various legal domains, including but not limited to intellectual property, consumer protection and data privacy. Whilst most jurisdictions are willing to acknowledge the commercial nature of these platforms, specific legal frameworks that govern virtual economics, in-game

6. Lessig, *Code and Other Laws of Cyberspace*.
7. Lessig, 43.
8. Brownsword and Yeung, *Regulating Technologies*, 5.
9. Brownsword and Yeung, 3.

transactions and player rights are still evolving. Issues such as loot boxes, virtual property ownership and gambling-like mechanics have prompted additional regulatory scrutiny in some regions. In addition, the extraterritorial nature of online gaming will pose challenges in how regulations may be enforced across borders. As virtual worlds increasingly intertwine with real-world economies and social interactions, regulators and lawmakers strive to strike a balance between innovation and safeguarding user rights, shaping the intricate legal fabric enveloping MMORPGs.

For example, one of the top emerging London-based technology and MMO startups, Talewind,[10] is creating some innovative user experiences for the Metaverse, using platforms such as Sandbox and Roblox. In our current version of the Internet, Talewind would need to navigate a plethora of cyberlaws that apply in the United Kingdom (UK), being a UK-based legal entity. As a starting point, data protection and privacy of users would be a paramount concern. Data protection would be governed under the UK Data Protection Act 2018, and the UK General Data Protection Regulation (GDPR). If users of Talewind are also located abroad, for example, in a European Union (EU) country, then the application of the EU GDPR is also attracted.[11] Collectively, these data protection laws would ensure the protection of any personal data of the users of the Talewind platform, with far-reaching consequences in the event the provisions are not complied with. If Talewind users are under the age of 18, then it is also incumbent to take into account other regulatory guidance, such as the UK's Council for Internet Safety guidance document titled *Safeguarding children and protecting professionals in early years settings: online safety considerations*.[12] In the meantime, the UK government is also presently negotiating the Online Safety Bill[13] through Parliament, which, if passed, would provide stronger protections for children online, as well as protect freedom of speech. In its present state, the Online Safety Bill offers users a triple shield of protection online.[14] The protection of privacy in the UK, on the other hand, is limited in these legislations – but offers protection through the tort of misuse of private information instead, with legal protections offered vis-à-vis Article 8 of the Human Rights Act 1998 (mirroring Article 8 of the European Convention on Human Rights).[15] A recent case that tested the limits of privacy laws in the UK is the case of the *Duchess of Sussex v Associated Newspapers Ltd*.[16]

New dimensions of criminality such as internet crimes and other forms of online harassment are also emerging problems in online and virtual spaces. With the rise of social media and other forms of social interactions such as dating applications, so, too, has arisen the phenomenon on 'sextortion', online blackmailing, threats to expose particularly private information, catfishing, defamation and the like. Research conducted by various law firms in the UK has revealed that defamation cases have tripled since 2016, particularly attributing this increase to postings on social media. Whilst the

10. 'Talewind Homepage', Talewind, Accessed 4 August 2023, https://talewind.co.uk/.

11. 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).

12. UK Council for Internet Safety, 'Safeguarding Children and Protecting Professionals in Early Years Settings: Online Safety Considerations', GOV.UK, February 2019, https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations.

13. 'Online Safety Bill', GOV.UK, 3 February 2023, https://www.gov.uk/government/collections/online-safety-bill.

14. 'New Protections for Children and Free Speech Added to Internet Laws', GOV.UK, 28 November 2022, https://www.gov.uk/government/news/new-protections-for-children-and-free-speech-added-to-internet-laws.

15. 'European Convention on Human Rights', n.d., 30.

16. [2021] EWCA Civ 1801.

case of *Depp v News Group Newspapers Ltd & Anor*[17] has dominated the spotlight over the last couple of years, other cases brought for defamation claims in the UK, such as *TJM v Chief Constable of West Yorkshire Police*[18] and *Dudley v Philips*[19] demonstrate the mettle of the law in handling social media defamatory claims. In connection with online harassment, cyber bullying and the like, whilst the UK Protection from Harassment Act 1997 and the enlarged purview of harassment in *Khorasandjian v Bush*[20] is quite limited in this instance, the regulatory dimensions of harassment have evolved quite positively in the UK context. For example, the civil case of *Kirat Assi v Simran Kaur Bhogal* resulted in an undisclosed substantial settlement for the longest and most elaborate catfishing scheme, even though catfishing is not recognized as a legal crime.

Whilst the above paragraphs have highlighted some key areas of legislation that apply as part of Internet governance, other aspects of the legal dimensions that need to be addressed in online and virtual platforms include various intellectual property rights (copyright and trademark), consumer protection laws, legitimacy of contractual arrangements, cybersecurity, advertising, competition laws and user interactions; and these also form part of the fragmented landscape in Internet laws and governance, which also apply to MMORPG platforms.

Governing DeSoc: Reconciling a paradox

Taking into consideration the realities that the Internet has created, a new question emerges as we begin to make the transition into Web3.0, a new version of the Internet that promises heightened user control and autonomy as its *pièce de resistance* and aims to introduce DeSoc as part of this scaffolding. It is likely that renewed legal issues may arise, for example, those relating to identifying and defining new modalities of use and interactions, jurisdictional matters and identification and enforcement of existing and 'new' legal rights.

In the first instance, we should identify what Web3.0 is and why it is touted to be superior to our current version of the Internet (Web2.0). Web3.0 in essence boasts a decentralized nature that would theoretically establish a more open, transparent and decentralized online and virtual environment for users – with its main selling point being elevated control and heightened user autonomy over their own data and information that might be shared with a network or community. In our current version of the Internet, known as Web2.0, we are typically inundated with platforms managed by technology companies, that although provide users with sophisticated services and goods, trades off on user data, security and control of the flow of personal information that is captured. Because Web3.0 relies on decentralized technologies such as blockchain, peer-to-peer networks and smart contracts, these technologies empower users to directly engage with other stakeholders in the community, without any intermediaries. These measures ensure heightened privacy, security and authority of users over their personal information. This is the cornerstone of a DeSoc, enabling a diverse array of decentralized applications capable of delivering novel services and encounters, such as decentralized finance, social networks and marketplaces. Though still nascent in its developmental stage, Web3.0 holds the potential to revolutionize interactions with each other and the global landscape.

17. [2020] EWHC 2911 (QB).
18. [2022] EWHC 2658 (KB).
19. [2022] EWHC 930 (QB).
20. [1993] QB 727.

The vision of Web3.0 and DeSoc has been the subject of a White Paper,[21] co-authored by, amongst others, the founder of Ethereum, Vitalik Buterin. With DeSoc being the main component of the White Paper, it was also recognized by the authors that there are challenges in achieving the construction of a true DeSoc. One of these is the necessity for adaptable property rights, what the authors refer to as 'decomposable property rights'.[22] Decomposable property rights involve the concept of breaking down a property right into its individual parts, such as the rights to use (usus), rights to consume or destroy (abusus) and rights of profits (fructus). In conventional property rights, these are bundled together. In DeSoc, however, it would be possible to separate these rights into components that can be owned and traded separately. Examples of this occurrence would be the virtual property bought in Snoop Dogg's Snoopverse[23] as well as professional services giant, Price Waterhouse Coopers buying virtual land in Sandbox.[24]

Because decomposable property rights (as one example) are markedly different from traditional property rights in law, there is question as to how decomposable property rights should be governed in the Metaverse. For example, traditional real property rights in England have had a long history of evolution, beginning from the Normandy invasion in 1066, evolving through the Law of Property Act 1925 where all free citizens (pursuant to the Magna Carta) could own and trade property. Property law is also multifaceted in real life, with property boundaries equally complex in nature.[25] Absent a process of evolution in the Metaverse, how is it to be decided, and who decides, which aspects of property law should apply? Virtual boundaries to be drawn are also challenging, prompting issues of inalienability of such property.

Other issues of DeSoc in the Metaverse relate to governance mechanisms and community-led administration. Decentralized Society focuses on governance powered by the community, by facilitating decentralized autonomous organizations (DAOs) that can offer clear and responsible governance for decentralized networks and applications. These DAOs are managed through smart contracts, allowing stakeholders to collaborate on decisions and voting without relying on central authorities. The conceptual nature of DAOs aside more inquiries need to be conducted into whether DAOs can ensure the protection of user rights and safety in Web3.0 and the Metaverse. In existing Web2 infrastructure, for example, governance is ensured (although not always completely reliably) through the rule of law, modern democratic values and with key legislation such as the GDPR and other forms of Internet laws that seek to protect users, competition and the market. Is it also therefore possible for DeSoc in virtual worlds and the Metaverse to be governed in a similar way? Is it counterproductive to the fundamental tenet of DeSoc, which is essentially to reject centralized governance? Are DAOs decentralized in nature, or only in title – and who appoints the DAOs? How are breaches enforced and sanctioned?

The problem with governance mechanisms of DAOs in Web3.0 is that they often rely on centralized Web2 infrastructure, such as social media profiles, for sybil resistance. Sybil resistance refers to the ability of a system to prevent individuals from creating multiplate fake identities in

21. Weyl, Ohlhaver, and Buterin, 'Decentralized Society'.

22. Weyl, Ohlhaver, and Buterin, 1.

23. Kylie Logan, 'Snoop Dogg Is Developing a Snoopverse and Someone Just Bought a Property in His Virtual World for Almost $500,000', *Fortune*, 9 December 2021, https://fortune.com/2021/12/09/snoop-dogg-rapper-metaverse-snoopverse/.

24. Consultancy.uk, 'PwC Buys Virtual Land NFT in the Sandbox's Metaverse', 4 January 2022, https://www.consultancy.uk/news/30011/pwc-buys-virtual-land-nft-in-the-sandboxs-metaverse.

25. Blomley, 'The Boundaries of Property', 224–55.

order to gain more influence or control over a system.[26] In a decentralized system such as DeSoc, it is important to have robust sybil resistance mechanisms that can prevent such attacks. However, many DAOs in Web3.0 rely on centralized social media profiles for sybil resistance, which can be vulnerable to manipulation and control by centralized entitles. This can undermine the decentralization and autonomy of the DAOs and make it more susceptible to capture or domination by external actors. Acknowledging this problem, DeSoc proposes enhanced governance mechanisms that reward trust and cooperation while protecting networks from capture and domination.[27] However, these are mostly theoretical in nature, with little evidence of real-world test uses enabling the verification and efficiency of such mechanisms. It would be prudent to proceed with caution until such time that a proper DeSoc regulatory framework can be established.

Platform power: Renegotiating EULAs in the Metaverse

One of the fundamental arguments regarding regulation and control in online and virtual spaces is inextricably linked to power, in this instance, specifically platform power. This is the key reasoning behind the intention of Web3.0, to transform those who wield platform power (often, big tech corporations and governments), in favour of collective user autonomy. The concept of platform power has increased in importance in scholarly lexicon – particularly that 'existing legal mechanisms do not adequately reflect the power over information flows and individual behaviors that gatekeepers can exercise'.[28] Besides the fact that 'digital gatekeepers render their operations impervious to scrutiny by individual users'[29] through specific measures such as complex technological design, or legal and technical jargon in user terms and conditions, so too becomes apparent that platform power in our technological epoch is synonymous with the 'microphysics of power', a key concept of Michel Foucault's technologies of power.[30] Power exercised over individuals by platforms are a distinct strategy, where 'its effects of domination are attributed not to appropriation, but to dispositions, maneuvers, tactics, techniques'.[31] However, whilst Foucault does not attribute this to a dominant class, it is evident that our reverberation of the Internet in its present form rests in the hands of the powerful corporate elites who have the capacity to exude control over its use.

Protection of users vis-à-vis *end user license agreements*

On MMORPG platforms, or any other platform on the Internet that offers digital goods or services, the EULAs is the pivotal agreement between an individual user and the platform provider / owner. End-User License Agreements are contractual instruments that broadly govern the applications in the online or virtual platforms, delineating terms and conditions and specific stipulations under which users are permitted to engage with the provided software or service. End-User License Agreements, in this respect, function as legal frameworks that define the permissible scope of

26. Platt and McBurney, 'Sybil in the Haystack', 34.

27. Weyl, Ohlhaver, and Buterin, 'Decentralized Society', 18.

28. Orla Lynskey, 'Regulating "Platform Power"', SSRN Scholarly Paper (Rochester, NY, 21 February 2017), 1, https://doi.org/10.2139/ssrn.2921021.

29. Lynskey, 1.

30. Foucault, *Discipline and Punish*.

31. Foucault.

usage, limitations of such use (e.g. prohibiting replication or distribution beyond personal use) as well as implications of breach or non-compliance with the terms and conditions.

End-User License Agreements play a pivotal role in safeguarding the interests of both end users and the respective software providers. They establish a delineation of user entitlements, delineating the boundaries within which software and services can be accessed and operated. This may encompass delineations of proprietary rights, usage permissions and potential constraints on reverse engineering or modification. These agreements address matters of data privacy and security, elucidating the way user data is collected, processed and potentially shared. End-User License Agreements theoretically also often inform users about the procedures for handling disputes or seeking remedies in case of conflicts arising from the software usage or its provisions. While often intricate and legally detailed, EULAs hold a distinct purpose in fostering transparency, managing user expectations and mitigating potential legal issues through formalized consent and adherence to defined norms.

Whilst EULAs ostensibly establish to afford users a degree of protection, it is always advisable for users to acquaint themselves with the contents of EULAs to ensure alignment with their preferences and to facilitate informed decision-making prior to engagement with software or online services. However, an in-depth examination of EULAs reveals some nuances that cast doubt upon the efficacy of EULAs in effectively safeguarding user interests.[32] In Table 1, some of the shortcomings in EULAs are highlighted in attempting to address the second question of this paper: whether EULAs can protect user interests in Web3.0.

In summation, while EULAs ostensibly proffer a structured framework for user engagement, their legitimacy in effectuating bona fide user protection remains susceptible to scrutiny. Their labyrinthine language, the inherent imbalance of negotiating power, overarching standardization and the proclivity for one-sided stipulations collectively conspire to engender an environment wherein user interests are frequently secondary to those of the software providers. The realization of genuine user protection necessitates a paradigm that prioritizes transparency, user-oriented comprehensibility and a negotiation landscape that equitably accommodates the concerns of both parties.

In existing Web2 infrastructure, EULAs may not adequately protect the rights of its users – it leaves to be seen if it can do so in Web3.0 and virtual worlds like the Metaverse. The reality is that if EULAs presently favour software or platform providers, there is little to demonstrate that it will change its stance to favour user interests or protections in Web3.0.

Renegotiating EULAs in the Metaverse

In the context of the emerging Web3.0 and Metaverse, the requisite re-evaluation and potential restructuring of EULAs become a compelling consideration. The distinctive intricacies of the Metaverse, characterized by immersive and interconnected digital environments, necessitate a departure from convention EULAs frameworks. With heightened emphasis on user agency, virtual identities and data integration, EULAs tailored for the Metaverse would likely need to adopt more user-centric, comprehensible language that accounts for the unique dynamics of this space. In this novel milieu, challenges manifest in specific ways. These include segmented concerns related to user data privacy and ownership within virtual spaces, the complex interplay of virtual economies and real-world transactions, evolving standards for digital property rights and the

32. Susan Corbett, 'Computer Game Licences: The EULA and Its Discontents', *Computer Law & Security Review* 35, no. 4 (1 August 2019): 453–61, https://doi.org/10.1016/j.clsr.2019.03.007.

Table 1. Author analysis on shortcomings of traditional EULAs on internet platforms.

No.	Problems	Analysis
1	Complex legalese and user engagement	EULAs are conspicuous for their prolixity and legal jargon, presenting a formidable cognitive barrier for the average user. As a consequence of this linguistic complexity, users tend to resort to cursory perusal or outright neglect of these agreements. This engenders a situation wherein users unwittingly lend assent to provisions whose import may elude their comprehension.
2	Asymmetrical negotiating leverage	EULAs are constructed upon a foundational power asymmetry that vests the software provider with a pronounced upper hand in the realm of negotiation. This essentially reduces the user to a position of acquiescence within the confines of a 'take it or leave it' dynamic. Such a paradigm hardly connotes informed consent and precludes users from asserting preferences, negotiating terms or contesting conditions that might be prejudicial to their interests.
3	Standardization and holistic pertinence	The ubiquity of EULAs engenders a propensity for their standardization to cater to a diverse user base. This propensity towards generality manifests in the promulgation of terms that are broadly applicable but which, at times, fail to adequately accommodate idiosyncratic user exigencies. Consequently, the inclusivity of EULAs is, paradoxically, concurrently their Achilles' heel, often rendering their provisions either overbroad or insufficiently comprehensive.
4	Unilaterally skewed provisions	The provenance of EULAs within the legal bastions of software providers confers upon them an inherent skew towards safeguarding corporate interests. This can materialize in provisions that circumscribe users' entitlements, either via mechanisms such as arbitration clauses that obviate conventional legal recourse or through disclaimers of accountability for data breaches and service disruptions. This unilateral construct invariably curtails users' capacity to hold providers accountable in the event of unfavourable eventualities.
5	Opacities in data governance and handling	While certain EULAs do make cursory allusions to the domain of data privacy and security, these references are often obfuscated within the labyrinthine texture of these agreements. The resultant lack of transparency concerning the modalities of data collection, utilization and sharing undermines informed user consent, and simultaneously nurtures an environment ripe for privacy concerns.
6	Linguistic inaccessibility	EULAs, composed in language typical of legal discourse, present a substantial hurdle to intelligibility for the lay user. This expository dissonance curtails informed decision-making and engenders misunderstandings vis-à-vis the substantive nature and extent of the contractual arrangement.
7	Curtailed negotiability	EULAs diverge from the archetype of conventional contracts by typically precluding the possibility of user-initiated negotiations. This inhibits users from accommodating specific requisites or preferences, a facet that is frequently indispensable for attaining congruence between the agreement and individual user prerogatives.

potential for algorithmic decision-making to impact user experiences.[33] Crafting EULAs that effectively address these challenges entails fostering transparency in data governance, delineating the intricacies of virtual property rights, ensuring fair governance of virtual economies and establishing mechanisms for user dress in instances of algorithmically mediated disputes. In essence, the Metaverse introduces an array of intricate considerations that necessitate a paradigm shift in EULA construction, thereby requiring a more responsive framework that aligns with the evolving dynamics of this immersive digital realm.

The advent of the Metaverse, therefore, ushers novel dimensions in the context of MMORPGs, encompassing multifaceted novelties in data dynamics, user interactions and cybersecurity.[34] In this paradigm, user engagement extends beyond conventional virtual realms, intertwining with real-world data streams, thus requiring reimagined data governance frameworks. Enhanced user interaction mechanisms, often underpinned by virtual reality interfaces, engender an intricate fabric of social dynamics, necessitating comprehensive sociotechnical analyses to comprehend the emergent forms of collaboration, conflict and identity negotiation.[35] Simultaneously, the Metaverse amplifies cybersecurity exigencies. The amalgamation of expansive virtual landscapes with intricate economic systems and personalized data repositories engenders diverse vectors for malicious activities, necessitating cybersecurity paradigms adept at safeguarding the integrity of both virtual and real assets.[36]

One of DeSoc's answers to the problems of cybersecurity and enhanced data protection and privacy is soulbound tokens (SBTs), presented as the change-maker for a fully decentralized Web3.0. In essence, SBTs (whose name was inspired[18] by 'soulbound' property from the wildly successful MMORPG, World of Warcraft) are non-transferable, NFTs on the blockchain that contains all types of information relating to an individual. These may include information relating to identity, reputation, medical history, education and all and any kind of information relating to said individual. The concept behind SBTs is that individuals in DeSoc exercise self-sovereign identity and decentralized identifiers. This approach allows users to control information used to verify their identities for websites, applications, online services and the like. Indeed, it is believed that SBTs should be the cornerstone of DeSoc, the latter being 'a co-determined sociality, where Souls and communities convene in a bottom-up way as emergent properties of each other to produce plural network goods across different scales'.[37] The potential existence of SBTs necessitates a different working of EULAs to protect users in the Metaverse.

Case study: Renegotiating EULA for Blizzard Entertainment Inc

In this section, taking into consideration the novelties illustrated in 'Renegotiating End User License Agreements in the Metaverse' section above, this paper attempts to provide a hypothetical envisioning of EULAs that would offer better protections for users of MMORPG platforms in the

33. Dwivedi et al., 'Metaverse beyond the Hype', 102542.

34. Dwivedi et al.

35. Dasdemir, 'A Brain-Computer Interface', 645–52.

36. Tom Taulli, 'Cybersecurity in the Metaverse Will Require New Approaches', eSecurityPlanet, 19 January 2023, https://www.esecurityplanet.com/trends/metaverse-security/.

37. 'Welcome to Web3: Identity, Soulbound Tokens, and Decentralised Society', Crypto.com, 30 September 2022, https://crypto.com/research/web3-identity-soulbound-tokens.

Metaverse, simultaneously answering the third question posed in this paper. This paper relies on the publicly available EULA of Blizzard Entertainment Inc. (Blizzard)[38] as a case study.

As preliminary discussions, the Recitals in the Blizzard EULA make it very clear that the user has to abide by binding arbitration as well as waives rights to class actions. Whilst Recitals of this nature are common in most EULA and MMORPG platforms, the lack of user autonomy, as detailed in 'Renegotiating End User License Agreements in the Metaverse' section, and the unequal footing of negotiation leverage, is inconsistent with the operation of DeSoc in a Web3.0 Metaverse. In the event this would be aligned with a DeSoc nature, there should be room for negotiations of user autonomy to an extent that would be acceptable by the platform provider. For instance, in the same way that decomposable property rights are a feature in DeSoc, it may be worth reflecting if a bundle of user rights could also have the same features as decomposable property rights, for Metaverse MMORPGs – allowing the negotiation of the bundle of user rights, and as appropriate subject to negotiation, severing or allowing some partial rights to subsist.

Another critical point to evaluate is that if the intention of DeSoc is to decentralize Web3.0 functions and operations – then it must also be rational to conclude that platform owners and providers operating in the Web3.0 and Metaverse space should be open to negotiation for terms and conditions of use, particularly where user data and monetization is concerned.[39] So far, whilst there has been some evidence of smaller tech businesses demonstrating their willingness to alter their business models in order to take advantage of a Web3.0 position, it leaves to be seen whether large tech companies such as Amazon, Netflix or Google are likely to do the same.[40] Nevertheless, futurist tech commentators are of the opinion that in the event large tech companies do not want to lose a significant market share of the Web3.0 market, they would eventually need to come to a form of compromise, or risk losing profit margins over time.

In the meantime, the following Table 2 highlights some key provisions from the Blizzard EULA and the author's attempts to provide a brief analysis of its shortcomings, and whether it may be suitable for a Web3.0 and Metaverse DeSoc framework, or require negotiation for use in a novel virtual space. For ease of purpose, any references to DeSoc in the table shall include references to Web3.0 and the Metaverse.

Based on the author's analysis in Table 2, it is likely that MMORPG platforms that intend to venture into the Web3.0 Metaverse space would need to consider updating the terms and conditions in their relevant EULAs. In addition to existing legal provisions that have been identified, the prospective integration of new and novel clauses is a plausible consideration, acknowledging the evolving landscape encompassing NFTs, virtual assets, and the distinct attributes of DeSoc that include decomposable property rights, SBTs and other sophisticated mechanisms and impending infrastructure currently absent from Web2 domains. These additions could serve as essential measures to tackle the distinctive legal and regulatory complexities affiliated with NFTs and virtual assets. Such clauses would be aimed at enlightening users about their entitlements and obligations concerning these assets. Platform providers might contemplate introducing clauses that elucidate the realm of ownership and transferability concerning NFTs and virtual assets. Additionally,

38. 'Blizzard End User License Agreement - Legal – Blizzard Entertainment', 31 May 2023, https://www.blizzard.com/en-us/legal/fba4d00f-c7e4-4883-b8b9-1b4500a402ea/blizzard-end-user-license-agreement.

39. Jeff Bell, 'Council Post: In Web 3.0, Data Ownership and Monetization Must Belong To Individuals', Forbes, Accessed 12 August 2023, https://www.forbes.com/sites/forbestechcouncil/2022/03/31/in-web-30-data-ownership-and-monetization-must-belong-to-individuals/.

40. Bell.

Table 2. Author analysis on key clauses in blizzard EULA requiring renegotiation in Web3.0 Metaverse and DeSoc.

Clause	Provision	Analysis
A(1)(i)	Children under 13 may not utilize an Account, the Platform, nor enter into this Agreement even with the consent of a parent or legal guardian. Account users 13 or older but under 18 or the age of majority where they live (a 'Child') must review this Agreement and the Privacy Policy together with your parent or guardian. If you are the parent or legal guardian of an Account user who is a Child, you also agree to be bound by this Agreement on the Child's behalf. In the event that you permit your Child to use an Account or the Platform (including any Game), you hereby agree to this Agreement on behalf of yourself and your Child, and you understand and agree that you will be responsible for all uses of the Account or the Platform by your Child whether or not any particular use was authorized by you. Parents/guardians are jointly and severally liable for all acts and omissions of their Child for all uses of the Account and Platform.	• The stipulation in question serves a dual purpose. Primarily, it functions to shield children below 13 years from accessing the platform, a precautionary measure aligned with prevailing industry norms. Such restrictions are commonly enforced across digital platforms to pre-empt exposure to potentially unsuitable content or interactions. • Concurrently, the clause allocates a measure of responsibility to parents or legal custodians in overseeing the agreement and privacy policy with minors aged 13–18. This requisition, however, may be intricate for parents unfamiliar with the contractual vernacular, potentially impeding their ability to comprehensively review the agreement. This predicament is compounded for those facing temporal constraints or lacking adequate resources for meticulous scrutiny. • The viability of this clause within the DeSoc framework hinges on multifaceted considerations. Central to this appraisal is the age demographic targeted by the platform, with alignment or disjunction with the clause being contingent on the intended audience's age range. • Equally pivotal is the nature of the content and interactions facilitated by DeSoc, as these would determine the gravity of potential harm necessitating such a provision. Additionally, assessing the efficacy of this clause demands an evaluation of the capacity and accessibility of parents or guardians to diligently dissect the agreement alongside their children. • Hence, the appropriateness of this clause within the DeSoc construct is contingent upon an intricate interplay of age demographics, content characteristics and the parental or custodial infrastructure available for meticulous agreement review.

(continued)

Table 2. (continued)

Clause	Provision	Analysis
A(1)(vii)	You agree to pay all fees and applicable taxes incurred by you or anyone using your Account. If you choose a recurring subscription for a Game, you acknowledge that payments will be processed automatically (e.g., debited from your Battle.net Balance or charged to your credit card) until you cancel the subscription or the Account. Blizzard may revise the pricing for the goods and services offered through the Platform at any time. YOU ACKNOWLEDGE THAT BLIZZARD IS NOT REQUIRED TO REFUND AMOUNTS YOU PAY TO BLIZZARD FOR USE OF THE PLATFORM, OR FOR DIGITAL PURCHASES MADE THROUGH THE PLATFORM, FOR ANY REASON, EXCEPT AS REQUIRED BY APPLICABLE LAW.	• The inclusion of this clause within the context of DeSoc exhibits a congruence with the platform's operational ethos, given its lucid delineation of protocols pertaining to remuneration and subscription levies for platform utilization. By affording users the prerogative to willingly undertake financial obligations encompassing fees and associated taxes, a comprehensive comprehension of the fiscal responsibilities incumbent upon platform use is fostered. • This clause further imparts insights into the paradigm of recurring subscriptions and automated payments, thereby offering a resourceful channel for users aspiring to perpetuate unhampered access to the platform or specific interactive components. • Furthermore, the clause duly acknowledges the prerogative of Blizzard to modify the pricing structures governing the platform's merchandise and services – a practice consonant with prevailing norms prevalent amongst digital platforms and service domains. • *However,* it is imperative to underline that the clause enunciates Blizzard's non-obligation to reimburse amounts disbursed for platform utilization or digital acquisitions effected via the platform, save instances mandated by pertinent legislations. • This dimension potentially introduces apprehensions for users dissatisfied with the platform's performance or individuals encountering technical impediments impinging upon the platform's envisioned functionality.

(continued)

Table 2. (continued)

Clause	Provision	Analysis
A(1)(viii)	Blizzard and its partners (such as marketing and analytics providers) shall have the right to monitor and/or record your communications when you use the Platform, and you acknowledge and agree that when you use the Platform, you have no expectation that your communications will be private. Blizzard shall have the right to disclose your communications for any reason, including: (a) to satisfy any applicable law, regulation, legal process or governmental request; (b) to enforce the terms of this Agreement or any other Blizzard policy; (c) to protect Blizzard's legal rights and remedies; (d) to protect the health or safety of anyone that Blizzard believes may be threatened; or (e) to report a crime or other offensive behaviour.	• The stipulation outlined herein could potentially elicit apprehensions pertaining to the realms of data safeguarding and user privacy within the ambit of DeSoc. The attribution of authority to Blizzard and its affiliates for the monitoring and/or recording of user communications within the platform has the potential to evoke concerns amongst users who perceive a compromise in their privacy rights. • This unease is further compounded by the stipulation's explicit assertion that users should not anticipate a reasonable expectation of privacy when utilizing the platform – an assertion that might disconcert individuals who place a premium on maintaining their personal privacy. • Moreover, the clause extends latitude to Blizzard to divulge user communications for diverse motives, encompassing adherence to extant laws or regulations, enforcement of agreement terms or auxiliary policies, fortification of Blizzard's legal entitlements and recourses and safeguarding the well-being of individuals ostensibly imperilled. • While some of these rationales could be construed as legitimate under specific contexts, the potential for user communications to be unveiled sans their prior acquiescence is a facet that might elicit user apprehensions regarding potential invasions of their privacy. • Holistically appraised, while this clause might align with the prerogatives of Blizzard's platform, its resonance within the DeSoc milieu – where emphasis on user privacy and data integrity is paramount – may be incongruent. • In this context, Blizzard should contemplate recalibrating this clause to furnish more explicit safeguards for user privacy and data. Such revisions could encompass augmenting the stringency governing the circumstances warranting the monitoring or disclosure of user communications, thereby ensuring a judicious equilibrium between platform functionality and users' privacy imperatives.

(continued)

Table 2. (continued)

Clause	Provision	Analysis
D(i)(3)	Advertising. The Platform may incorporate third-party technology that enables advertising on the Platform and/or in certain Games playable on the Platform, which may be downloaded temporarily to your personal computer and replaced during online game play. As part of this process, Blizzard and/or its authorized third party advertisers may collect standard information that is sent when your personal computer connects to the Internet including your Internet protocol (IP) address.	• The present stipulation potentially engenders apprehensions concerning privacy and the attainment of consent within the DeSoc framework. Through the assimilation of third-party technology facilitating advertising within the platform and/or specific games, users may harbour concerns regarding the unsanctioned collection and utilization of their personal data. • This circumstance can be exacerbated by the provision's revelation that fundamental information, such as the user's IP address, is susceptible to collection upon the user's personal computer connecting to the internet – eliciting qualms amongst privacy-conscious users. • Nonetheless, the clause lacks explication pertaining to the modality of user data utilization or sharing, be it by Blizzard or its duly authorized third-party advertisers. • It is imperative for DeSoc to imbue its discourse with lucid and transparent elucidations detailing the processes of user data acquisition, application and dissemination. Concurrently, the acquisition of user consent assumes a pivotal role in these activities. • Whilst this clause may find consonance within the purview of Blizzard's platform, its harmony with DeSoc, oriented towards user privacy and volitional consent, is disputable. • As such, it would be prudent to contemplate a revision of this clause, characterized by an amplification of elucidations surrounding the collection, utilization and sharing of user data, alongside a robust mechanism to solicit user consent for these operations, particularly in connection with far-reaching legislation such as the European Union General Data Protection Regulation.

(continued)

Table 2. (continued)

Clause	Provision	Analysis
D(i)(4)	User Created or Uploaded Content. The Platform may provide you an opportunity to upload and display content on the Platform, such as on the Blizzard forums, and/or as part of a Game, including the compilation, arrangement or display of such content (collectively, the 'User Content'). User Content specifically does not include a Custom Game, as defined in Section 1.D.ii.1. below. You hereby grant Blizzard a perpetual, irrevocable, worldwide, fully paid up, non-exclusive, sub-licensable, right and license to exploit the User Content and all elements thereof, in any and all media, formats and forms, known now or hereafter devised. Blizzard shall have the unlimited right to copy, reproduce, fix, modify, adapt, translate, reformat, prepare derivatives, add to and delete from, rearrange and transpose, manufacture, publish, distribute, sell, license, sublicense, transfer, rent, lease, transmit, publicly display, publicly perform, provide access to, broadcast and practice the User Content as well as all modified and derivative works thereof and any and all elements contained therein, and use or incorporate a portion or portions of the User Content or the elements thereof in conjunction with or into any other material. [Full clause available online]	• This stipulation elicits potential concerns pertaining to intellectual property rights within the DeSoc realm. By conferring upon Blizzard an enduring, unalterable, worldwide, fully remunerated, non-exclusive and sub-licensable entitlement and license to exploit user-generated content and its constituent elements, users may perceive an acquiescence to relinquish their intellectual property rights sans adequate compensation or regulatory agency over the utilization of their content. • Moreover, the clause's omission of unequivocal information regarding the manner in which user-generated content will be employed or shared by Blizzard is a factor that could disconcert users who aspire to maintain dominion over their intellectual property. • The onus rests on DeSoc to furnish unambiguous and transparent insights into the utility of user-generated content, coupled with the securing of user authorization for these operations. • Nevertheless, an exception catering to Custom Games, as delineated in Section 1.D.ii.1, offers a semblance of assurance to users endeavouring to retain control over their intellectual property within the precincts of custom games. • The compatibility of this clause with Blizzard's platform notwithstanding, its resonance within the DeSoc domain – marked by an accentuated emphasis on user intellectual property rights – evokes scepticism. • In this context, it would be well-advised to deliberate upon a redaction of this clause, characterized by a more expansive delineation of the applications of user-generated content and the solicitation of user authorization for these activities. • Additionally, Blizzard would benefit from devising explicit safeguards for user intellectual property rights, particularly within the custom games framework.

(continued)

Table 2. (continued)

Clause	Provision	Analysis
D(ii)(3)	Pre-Loaded Software The Platform may contain additional software that requires you to agree to additional terms prior to your use thereof ('Additional Software'). A. Installation. You agree that Blizzard may install Additional Software on your hard drive as part of the installation of the Platform, and from time to time during the term of this Agreement. [Full clause available online]	• This provision bears relevance within the framework of DeSoc, as it furnishes insights into the prospect of supplementary software being integrated into the platform and the concomitant requisites users must adhere to. By stipulating that the platform might encompass supplementary software necessitating user compliance with additional terms prior to usage, the users are duly alerted to the possibility of supplementary obligations or constraints accompanying platform utilization. • The clause also specifies Blizzard's prerogative to introduce supplementary software into the user's hard drive during platform installation and intermittently throughout the agreement's duration. This implies that users might be necessitated to concur with supplementary terms or restrictions for software usage. • However, it remains imperative to acknowledge that the clause could be deemed arbitrary if the supplementary software bundled with the platform does not substantively contribute to user platform access or utilization. In such instances, the imposition of supplementary terms or constraints for software usage might be construed as capricious or inequitable. • Blizzard must meticulously ensure that any supplementary software embedded within the platform serves an indispensable purpose for user access or utilization. Furthermore, any supplemental terms or restrictions related to this software must remain rational and requisite. • Blizzard might contemplate revising this clause to proffer more precise insights into the categories of supplementary software that might be integrated with the platform, in addition to ensuring user awareness of any supplemental requisites or constraints associated with the said software.

(continued)

Table 2. (continued)

Clause	Provision	Analysis
D(ii)(4)	Consent to Monitor. WHILE RUNNING, THE PLATFORM (INCLUDING A GAME) MAY MONITOR YOUR COMPUTER, CONSOLE, OR MOBILE DEVICE'S MEMORY FOR UNAUTHORIZED THIRD PARTY PROGRAMS RUNNING EITHER CONCURRENTLY WITH A GAME OR OUT OF PROCESS. AN 'UNAUTHORIZED THIRD PARTY PROGRAM' AS USED HEREIN SHALL BE DEFINED AS ANY THIRD PARTY SOFTWARE PROHIBITED BY SECTION 1.C. ABOVE. IN THE EVENT THAT THE PLATFORM DETECTS AN UNAUTHORIZED THIRD PARTY PROGRAM, (a) THE PLATFORM MAY COMMUNICATE INFORMATION BACK TO BLIZZARD, INCLUDING WITHOUT LIMITATION YOUR ACCOUNT NAME, DETAILS ABOUT THE UNAUTHORIZED THIRD PARTY PROGRAM DETECTED, AND THE TIME AND DATE; AND/OR (b) BLIZZARD MAY EXERCISE ANY OR ALL OF ITS RIGHTS UNDER THIS AGREEMENT, WITH OR WITHOUT PRIOR NOTICE TO THE USER. [Full clause available online].	• This clause could raise reservations regarding its suitability for DeSoc, particularly with respect to privacy, data protection and informed consent. The clause's stipulation of monitoring the memory of a user's computer, console or mobile device for unapproved third-party software has the potential to amass sensitive user information without their awareness or acquiescence, thereby invoking privacy concerns. • Moreover, the absence of transparent elucidation regarding how this acquired data will be utilized or shared by Blizzard introduces uncertainty that might unsettle privacy-conscious users. • Additionally, the clause specifies the potential transmission of information back to Blizzard, encompassing the user's account name, particulars of the identified unauthorized third-party program and the associated timestamp. This element could elicit disquiet amongst users' intent on retaining dominion over their personal data, who might eschew its dissemination to external entities. • In an encompassing assessment, while this clause might harmonize with Blizzard's platform, its congruence with DeSoc – an entity accentuating user privacy and informed consent – is questionable. • Blizzard should contemplate a clause revision marked by comprehensive disclosures delineating the scope of data collection, application and sharing, alongside the attainment of user assent for these processes. • Moreover, Blizzard should mull over the implementation of augmented safeguards preserving user privacy, particularly within the purview of monitoring user conduct and detecting unapproved third-party software.

(continued)

Table 2. (continued)

Clause	Provision	Analysis
D(ii)(5)	Limited Warranty. TO THE FULLEST EXTENT ALLOWED BY APPLICABLE LAW, THE PLATFORM, ACCOUNTS, AND THE GAME(S) ARE PROVIDED ON AN 'AS IS' AND 'AS AVAILABLE,' BASIS FOR USE, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF CONDITION, UNINTERRUPTED OR ERROR-FREE USE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, TITLE, AND THOSE ARISING FROM COURSE OF DEALING OR USAGE OF TRADE, and the entire risk arising out of use or performance of the Platform and the Game(s) remains with the user. [Full clause available online].	• The inclusion of this clause within the framework of DeSoc emerges as apt, considering its articulation of disclaimers pertaining to warranties and constraints on liability, delimited by the permissible purview of prevailing jurisprudence. By elucidating that the platform, accounts and games are offered on an 'as is' and 'as available' basis, bereft of any form of warranty, users are apprised of their assumption of inherent risks in their engagement with the platform and associated games. • Simultaneously, the clause expressly abnegates any implicit warranties, encompassing conditions of uninterrupted or error-free usage, marketability, appropriateness for specific objectives, non-infringement, title and those derivative of conventional transactional practices or trade conventions. This provides a measure of assurance to users apprehensive about the calibre or efficacy of the platform and games. • It is, however, imperative to underline that the clause does not engender an all-encompassing exemption from liability for all categories of losses or damages. The clause asserts the immunity of Blizzard, its parent company, subsidiaries, licensors and affiliates from accountability pertaining to losses or damages incurred due to user utilization or the incapacity to access or engage with the platform or accounts, except within the bounds delineated by express statutory demarcations. • This underscores the potential existence of specific categories of damages or losses that might remain immune to exclusion as prescribed by law, thus entailing that users might retain legal recourse under certain circumscribed scenarios. • Whilst this clause aligns with the contours of DeSoc, it is of paramount import for Blizzard to ensure full compliance with the extant legal edifice governing warranties and liability limitations. It might contemplate a clause revision encompassing an elaborate enunciation of the gamut of damages or losses susceptible to lawful exclusion. Additionally, it is incumbent upon the provider to secure that users are cognizant of their legal entitlements and remedies, thereby fostering a milieu of transparency and legal alignment.

(continued)

Table 2. (continued)

Clause	Provision	Analysis
11	CLASS AND COLLECTIVE ACTION WAIVER. TO THE FULLEST EXTENT ALLOWED BY APPLICABLE LAW, YOU AND BLIZZARD AGREE THAT EACH PARTY MAY BRING DISPUTES AGAINST THE OTHER PARTY ONLY IN AN INDIVIDUAL CAPACITY, AND NOT AS A CLASS ACTION, COLLECTIVE ACTION OR CLASS ARBITRATION, OR AS A PRIVATE ATTORNEY GENERAL. To the extent applicable law does not permit waiver of private attorney general claims, but permits them to be arbitrated, then such claims shall be resolved in arbitration. The arbitrator shall be empowered to grant whatever relief would be available in a court under law or in equity.	• This stipulation holds potential validity within the framework of DeSoc, being a contractual accord between the user and Blizzard addressing the resolution of conflicts. The clause expounds that either party can raise disputes against the other solely on an individual basis, precluding the instantiation of collective actions, class actions, class arbitration or the role of a private attorney general. • This essentially signifies that users cannot institute claims against Blizzard collectively, but must instead pursue claims individually. • It is crucial, however, to underscore that the clause's efficacy is delimited by the scope of applicable law. If prevailing legislation prohibits the relinquishment of private attorney general claims, yet permits their arbitration, such claims shall be redressed via arbitration. • In effect, this signifies that users might retain the avenue to institute private attorney general claims through the medium of arbitration, should statutory provisions so allow. • Whilst this clause could align with DeSoc, it is incumbent upon DeSoc to ensure strict adherence to the diverse legal norms and regulations governing the domains of dispute resolution and waivers of class actions. • Parties might deliberate upon a clause revision characterized by an enhanced articulation of the categories of claims amenable to arbitration, alongside guaranteeing user cognizance of their legal entitlements and recourses. Furthermore, parties should consider formulating more explicit safeguards for users encountering impediments in pursuing claims individually, especially within the context of private attorney general claims.

addressing the attendant risks linked to these assets, such as potential loss or theft, could be imperative. Another facet that providers should consider encompasses clauses delving into the application of virtual assets within the platform. These could include stipulations outlining restrictions against their illicit or unauthorized utilization.

Conclusion

Ensuring that EULAs align with the distinctive attributes of Web3.0, the Metaverse and DeSoc holds considerable significance, as these nascent technologies and platforms introduce novel legal and regulatory complexities that may surpass the purview of conventional EULAs. By imbuing EULAs with reflections of these distinctive attributes, a safeguard is established to enlighten users about their rights and obligations within the context of these technologies and platforms, concurrently offering guidance on their judicious and responsible utilization.

To illustrate simply, the distinct nature of Web3.0, the Metaverse and DeSoc is underscored by their reliance on blockchain technology, NFTs and virtual assets. These elements introduce legal and regulatory challenges encompassing ownership, transferability and security. Tailored EULAs can impart awareness of the associated risks to users and furnish guidance to mitigate these risks. Moreover, these entities are characterized by user-generated content, social features and community guidelines, each laden with unique legal and regulatory intricacies involving content moderation, privacy and data protection. Reflective EULAs can ensure users' comprehension of their entitlements and duties pertaining to these components, offering direction for usage that respects fellow users' rights and aligns with applicable legal frameworks. This is the way forward in the event we truly wish to exemplify user autonomy and protections.

Ultimately, EULAs that mirror the distinct features of Web3.0, the Metaverse and DeSoc fulfil a pivotal role in acquainting users with the distinct legal and regulatory quandaries inherent in these emergent technologies and platforms. Furthermore, they provide users with guidelines for their safe and responsible use. This proactive stance engenders user confidence and trust in these technologies and platforms, thus fostering their adherence within the parameters of legality and social responsibility. Whilst it is still early days before Web3.0 and the Metaverse become mainstream technologies, seeking counsel from legal professionals and industry specialists is advised to ascertain the requisite clauses for the EULA's comprehensive efficacy, operational soundness and conformity with prevailing legal standards, and a robust adaptability to ensure protections in a new and novel space.

Declaration of conflicting interests

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Pin Lean Lau https://orcid.org/0000-0002-2447-9293

References

'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)', n.d., 88.

Bell, Jeff.. 2022. *Council Post: In Web 3.0, Data Ownership And Monetization Must Belong To Individuals*. Jersey City, New Jersey, United States: Forbes. Accessed 12 August 2023. https://www.forbes.com/sites/forbestechcouncil/2022/03/31/in-web-30-data-ownership-and-monetization-must-belong-to-individuals/.

Blizzard End User License Agreement - Legal – Blizzard Entertainment. 31 May 2023. https://www.blizzard.com/en-us/legal/fba4d00f-c7e4-4883-b8b9-1b4500a402ea/blizzard-end-user-license-agreement.

Blomley, Nicholas. 2016. "The boundaries of property: Complexity, relationality, and spatiality." *Law & Society Review* 50 (1): 224–255. https://www.jstor.org/stable/44122505. https://doi.org/10.1111/lasr.12182

Brownsword, Roger, and Karen Yeung. 2008. *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*. Oxford: Hart Publishing.

Consultancy.uk. 'PwC Buys Virtual Land NFT in the Sandbox's Metaverse', 4 January 2022. https://www.consultancy.uk/news/30011/pwc-buys-virtual-land-nft-in-the-sandboxs-metaverse.

Cooper, Peter. 'WEB 3.0 Impact on the Business and Legal Issues'. Fintech Harbor Consulting, 3 October 2022. https://www.fintecharbor.com/web-3-0-impact-on-the-business-and-legal-issues/.

Corbett, Susan. 2019. "Computer game licences: The EULA and its discontents." *Computer Law & Security Review* 35 (4): 453–461

Crypto.com. 'Welcome to Web3: Identity, Soulbound Tokens, and Decentralised Society', 30 September 2022. https://crypto.com/research/web3-identity-soulbound-tokens.

Dasdemir, Yasar. "A brain-computer interface with gamification in the metaverse." *Fayoum University Journal of Engineering* 13 (3 January 2023): 645–652. https://doi.org/10.24012/dumf.1134296.

Dwivedi, Yogesh K., Laurie Hughes, Abdullah M. Baabdullah, Samuel Ribeiro-Navarrete, Mihalis Giannakis, Mutaz M. Al-Debei, Denis Dennehy, et al. 2022. "Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy." *International Journal of Information Management* 66: 102542.

European Convention on Human Rights. n.d. 30.

Foucault, Michel. 1977. *Discipline and Punish: The Birth of The Prison*. New York: Vintage Books, Random House.

GOV, U. K. 'New Protections for Children and Free Speech Added to Internet Laws', 28 November 2022. https://www.gov.uk/government/news/new-protections-for-children-and-free-speech-added-to-internet-laws.

GOV, U. K. 'Online Safety Bill', 3 February 2023. https://www.gov.uk/government/collections/online-safety-bill.

Lau, Pin Lean. 2022. "The murky waters of the metaverse: Addressing some key legal concerns." *Communications Law* 27 (2): 76–83.

Lessig, Lawrence. 1999. *Code and Other Laws of Cyberspace*. New York: Basic Books.

Logan, Kylie. 'Snoop Dogg Is Developing a Snoopverse and Someone Just Bought a Property in His Virtual World for Almost $500,000'. *Fortune*, 9 December 2021. https://fortune.com/2021/12/09/snoop-dogg-rapper-metaverse-snoopverse/.

Lynskey, Orla. 'Regulating "Platform Power"'. SSRN Scholarly Paper. Rochester, NY, 21 February 2017. https://doi.org/10.2139/ssrn.2921021.

Platt, Moritz, and Peter McBurney. 2023. "Sybil in the haystack: A comprehensive review of blockchain consensus mechanisms in search of strong sybil attack resistance." *Algorithms* 16 (1): 34.

Polkadot.ERI. 'One Article to Understand The Past, Present, and Future of Web 3.0'. *Polkadot Network* (blog), 7 December 2021. https://medium.com/polkadot-network/one-article-to-understand-the-past-present-and-future-of-web-3-0-5433962b7c3e.

Robson, Kurt. 'Gaming Industry to Be Worth $470bn by 2030 despite Setbacks, Experts Predict'. *Verdict* (blog), 3 April 2023. https://www.verdict.co.uk/gaming-industry-to-be-worth-470bn-by-2030-despite-setbacks-experts-predict/.

Talewind. 'Talewind Homepage'. Accessed 4 August 2023. https://talewind.co.uk/.

Taulli, Tom. 'Cybersecurity in the Metaverse Will Require New Approaches'. eSecurityPlanet, 19 January 2023. https://www.esecurityplanet.com/trends/metaverse-security/.

UK Council for Internet Safety. 'Safeguarding Children and Protecting Professionals in Early Years Settings: Online Safety Considerations'. GOV.UK, February 2019. https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations.

Weyl, Eric Glen, Puja Ohlhaver, and Vitalik Buterin. 2022. "Decentralized Society: Finding Web3's soul." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4105763.

Author biography

Pin Lean Lau is a Senior Lecturer (Associate Professor) of Bio-Law. A former practising barrister and solicitor, she was a corporate-commercial attorney working primarily in corporate finance, mergers and acquisitions, cyber and technology law, and general corporate advisory matters. Her signature research straddles the intersection of law, technologies (existing and emerging), science, ethics, and society. Her current research encompasses European, international and comparative law for legal governance and regulatory frameworks of technologies using a human rights & intersectional lens, specifically in artificial intelligence and feminist approaches in health and medicine (including medical devices); reproductive & biomedical and health technologies; genome editing technologies; ectogenesis in extreme extraterrestrial environments; virtual worlds (Metaverse) & legal complexities of DeSoc & soulbound tokens; health & medicine in the Metaverse including digital twins and telehealth; and technologies horizon scanning and futures- foresighting.