SUPREMO AMICUS

VOLUME 33 | JUNE, 2023 ISSN 2456-9704

METAVERSE UNVEILED: NAVIGATING DEVELOPMENT, LEGAL IMPLICATIONS, AND ADDRESSING SEXUAL HARASSMENT ISSUES WITHIN THE VIRTUAL FRONTIER

By Devansh Kulshreshtha
From NMIMS, Navi Mumbai

Abstract:

From cyber behemoths like Meta and Microsoft to Apple and IBM, everyone is laying the groundwork for a future where internet contact takes place predominantly in virtual worlds.

Concepts like blockchains aren't new until and unless someone has been living under a rock. The expeditious momentums NFTs, Meta, block-chains, and crypto-currency have been gaining not only hint at us but also push us in the direction of adaptation of Web 3.0. We, as a high-functioning society of intellects, are currently in the transition phase of technology, where we are moving forwards from Web 2.0 towards Web 3.0. Web 3.0 provides a peer-to-peer approach with decentralized blockchains. What this implies is that this format not only provides users with what can be publicized but also gives them access to preserve and store information, secretly. With this distributed ledger, its users are provided with a consistent and transparent method of storing data.

Technology rarely achieves just what it was meant for. With the upside to Meta-verse and Web 3.0, there exists a flip side. Currently, our IT laws aren't sufficient enough to suffice the present generation of technology. The momentum gained by Meta circles around the hard-hitting questions of privacy and safety. Due to the Westernized approach of Meta, the real issues lie before the international community- How has the international legal system adapted after the introduction of GDPR, and how an 1886 convention [***The Berne Convention***] is applicable in the digital era?

This article discusses how cyberbullying is progressively making its way into the virtual world. Many individuals believe that the meta-verse has the potential to blur the boundaries between reality and virtual reality. The sensory experience is heightened in a constant, all-encompassing digital environment, which exacerbates the sense of harassment, assault, cyberbullying, and hate speech.

INTRODUCTION TO META THROUGH WEB 3.0

Web 3 is a new version of the internet based on peer-to-peer and decentralized blockchains[1]. This format will provide users control over what is publicized, preserved, and secretly stored. A blockchain is a database that is hosted by a network of computers rather than a single server. This distributed ledger provides its users with a consistent and transparent method of storing data.

[1] Mangada, E. *The metaverse challenges and regulatory issues - sciences po*, *Science Po*. Available at: https://www.sciencespo.fr/public/sites/sciencespo.fr.public/files/Metaverse-Group-report-final-draft-June-12-1.pdf (Accessed: 09 June 2023).

The metaverse is a hot issue in today's modern world. From cyber behemoths like Meta and Microsoft to Nike and Tinder, everyone is laying the groundwork for a future in which internet contact takes place predominantly in virtual worlds. The Metaverse has enormous future potential, but with new worlds, new ideas, and new experiences, as well as extending what Roblox and Minecraft have to offer to new heights, there are hazards such as cyberbullying, privacy, harassment, safety, and more.

Many individuals believe that the metaverse has the potential to blur the boundaries between reality and virtual reality. This experience comes at a cost of constant surveillance on devices and unnecessary storage of data. This article aims to discuss the legal framework regarding data privacy and ownership.

LAWS RELATING TO META VERSE

1.1 GDPR

The EU introduces GDPR in 2018 and it dramatically changes the data privacy scenario for the better[2]. Under this regulation, EU residents can demand an organization who has stored their data to delete it and they are obligated to do so[3]. Any organization which collects, manages or stores information is obligated to abide by the user's request for deletion. It applies even to those organizations which don't function in the EU zone and they collect data. After GDPR similar legislations are being framed in Brazil, California, and Singapore. Articles 12-23 talk about data privacy and Article 54 talks about data stored by third parties.

VR and Glasses would make a big part of Web 3.0, such devices have the potential to store crucial data of the user such as eye movement, breathing patterns, and even brainwaves, this data could be used to influence user decisions and show targeted ads. GDPR is the only legislation that can restrict such storage of data.

1.2 THE BERNE CONVENTION

The Berne Convention gives producers such as authors, composers, poets, painters, and others the capability to decide how, by whom, and on what terms their art is used. It was formed in 1886 and has been ratified by 181 nations. It is based on 3 main principles and comprises a series of rules specifying the minimum protection to be offered.

It requires contractual parties to give full credit and rights to the respective owners, regardless of the method of expression.

So, the next question is how an 1886 convention is applicable in the digital era.

Other international accords, such as the WIPO copyright treaty, which was enacted in 1996, have been added to the convention, further connecting it to GDPR.

Because the metaverse is only a virtual reality, it will collide with real-world

[2] Cyber Bullying Research *centre Available at https://cyberbullying.org/metaverse] (Last visited on 19/1/2023)*

[3] [3] Tenkhoff, C., Kropp, J.A. and Rektorschek, J.P. (2022) *The metaverse: Legal challenges and opportunities*, *Lexology*. Available at: https://www.lexology.com/library/detail.aspx?g=c1872705-ccbe-49bb-98f4-77092e4f26ec (Accessed: 09 June 2023).

intellectual property rights, which are fundamentally territorial.

For example, UK trademarks cover the United Kingdom, while EU trademarks cover EU member states, however, this does not apply in the virtual world.

"A corpus of case law has evolved over time to attempt to tie IP infringement in the online realm to the physical world." This legal principle is known as targeting."

"However, there are requirements to determine 'where' the violation is occurring, at least under UK/EU legislation, and some facts and signs, such as currency or a website domain, may not even be present in a metaverse." With the rise of NFTs and individuals utilizing them to buy land, property, or even clothing in the metaverse, as well as develop their own virtual worlds and content, there will be numerous difficulties with ownership and how it is recorded.

Because there are several metaverses, transporting objects purchased or generated in one virtual world to another will result in intellectual property (IP) concerns[4].

DATA PRIVACY REGIME IN METAVERSE

Data security and privacy are important components of the Metaverse. Last year, when Metaverse announced its new set of Privacy Policies, there was widespread public outrage as individuals began to question the quantity of personal data that Metaverse would gather from their VR activities. In contrast, the overall intricacy of the notion reveals how complicated the Data Security activities would be behind this.

Metaverse is being developed to collect as much personal data as possible from users and then use that data to curate personalized products and services without requiring prior consent from anybody. Meta aims to collect data such as physiological responses, analyze eye movement, and record breathing patterns when the user is shown a certain type of advertisement. Not only recording this data is a problematic task but protecting this is an even bigger problem, data is generated in real-time while a user is exploring meta it is prone to be misused by hackers and malware attacks.

As of now as there is no law relating to avatars, the content which is explored by an avatar can result in the breaching of the personal details of a real-world person which further make them known.

NFTs are going to play a vital role as the majority of the transactions take place through NFTs. Since every individual NFT is linked to an individual virtual asset, any attack such as a cyber-attack may result in the loss of NFT-related data.

When it comes to sensitive data like the identity and wealth details of users, privacy is a major worry, and Data Security is attempting to keep the obtained data secure and away from being exploited. To help keep users' data safe from the operations team, a one-dimensional software like

[4] Palmer, J. (2022) *Copyright in the metaverse*, *Lexology*. Available at: https://www.lexology.com/library/detail.aspx?g=923 2e4d0-596b-4de3-bf5c-15c127d59427 (Accessed: 09 June 2023).

WhatsApp features a complicated double-layer end-to-end encryption security mechanism. As complicated as it may appear, the more sensitive and secret data a technology gathers, the more vulnerable it is to data theft and cyber hacking. Data security should be the main priority for Metaverse operators and data handlers. Meta has declared that it would collaborate with civil rights organizations to guarantee that personal data remains fundamental and powerful in the metaverse. There have been attempts to develop additional similar versions in which consumers would have better privacy and control over their personal data.

Security in Meta is important for the following reasons

1. Because the Metaverse is based on NFTs, it is vulnerable to NFT fraud.
2. In the future, blockchain-related scams and frauds are increasingly likely to develop.
3. Malware and data breaches may propagate.
4. The most susceptible data here is sensitive information such as a user's fingerprints.
5. Metaverse data security is all about protecting susceptible data from loss or theft. Meta was fined 405 million pounds for allowing children aged 13 to 17 for running business accounts on Instagram. This amount was the second-largest fine under GDPR

METAVERSE EXPERIENCE LABELLED AS "UNCOMFORTABLE"

A female journalist described her metaverse contacts as "uncomfortable" owing to a lack of etiquette guidelines in these areas, while another described them as "unnerving" due to the unexpected and hazardous nature of certain rooms.

The metaverse is being developed by many corporations with various measures in place to avoid interpersonal victimization, but when individuals are inevitably targeted and hurt, standards, and norms must be in place - and rigorously followed. To that end, each virtual environment must include a solid (and often updated) set of Community Guidelines to specify behavioral standards and to announce the presence of disciplinary processes for violations of conduct. On Meta, hundreds of content moderators flag hate speech posts or posts which are not suitable for public disinformation, and other violations, using text-reading algorithms. However, controlling behavior in virtual reality is far more difficult, both computationally and physically.

Contact theory gives the impression that individuals are more accepting when they meet someone face to face and can communicate verbally or can look in the eyes of the person in real-time. Is it feasible that people will just be kinder to one another in the metaverse?

The co-founder of meta-research claims that she was assaulted by a group of male avatars within a minute she joined the platform, one such instance happened with a researcher who joined meta to study user behavior, she was assaulted within hours of joining the platform[5].

[5] Basu, T. (2022) *The metaverse has a groping problem already*, *MIT Technology Review*. Available at: https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/ (Accessed: 07 June 2023).

While metaverse is being developed by certain applications, Facebook's metaverse refers to two major VR apps. Horizon Worlds, a networking program that allows users to communicate with other users in unique digital rooms, is one example. Venues, on the other hand, is committed to presenting virtual live-streaming events. Horizon Worlds and Venues are both accessible via Oculus VR headsets.

When a user in the metaverse is touched by another, the hand controllers vibrate, "producing an extremely unsettling and even unpleasant physical feeling during a virtual assassination." The watchdog also stated that "on a variety of applications, VR users have long experienced difficulties with sexual harassment, verbal abuse, racist insults, and violation of personal space."

In these VR settings, "little moderation" has allowed troubling conduct to "thrive... particularly towards female-appearing and female-sounding avatars."

CONCLUSION & SUGGESTION

Although life in the Metaverse appears to be exhilarating, additional obstacles exist. These include the problem of Metaverse Data Security. Self-protection and keeping software up to date Suffice it to say, these are the requirements of the virtual era.

Businesses must make an effort to restore the balance of power between themselves and their customers. In reality, this means providing people more say over how their information is used and processed.

"When it comes to data, particularly personal information, today's consumer-organization relationship is highly unbalanced." This is because developers and application owners have practically complete control over its collection, usage, and access.

It is advised that we accelerate the usage of frameworks such as Zero-Copy Integration and encourage developers to employ technologies like data ware and blockchain to minimize data and decrease copies so that the proper owner can manage it.

In reaction to assaulting of female avatars, Meta, for example, has proposed using a tool called "Safe Zone," a safety feature integrated into its Horizon Worlds. When the "Safe Zone" function is enabled, a virtual border is imposed that restricts avatars from approaching one other within a certain distance, reportedly making it simpler for users to avoid unpleasant encounters. While the EU's GDPR was implemented to curb the issue of data regulations throughout the European Union, it is unclear who, if anybody, would control the metaverse.

Data privacy issues multiply when intellectual and legal issues are integrated into it. Attempting to adapt present laws to the metaverse environment will be a huge task. From a regulatory standpoint, there will never be a single 'metaverse legislation' that attempts to cover everything, just as there is no one-stop single 'internet law,' since it just does not make sense. People are attempting to figure out how to apply and construct a proper regulatory environment based on the present framework.

"Undoubtedly, building meta will come first, the real legal difficulty will be determining how it is truly regulated".

*****