

In the Coming ‘Metaverse’, There May Be Excitement but There Certainly Will Be Legal Issues

New Media and Technology Blog on December 3, 2021

The concept of the “metaverse” has garnered much press coverage of late, addressing such topics as the new appetite for [metaverse investment opportunities](#), a recent [virtual land boom](#), or just [the promise of it all](#), where “[crypto, gaming and capitalism collide](#).”

The term “metaverse,” which comes from Neal Stephenson’s 1992 science fiction novel “Snow Crash,” is generally used to refer to the development of virtual reality (VR) and augmented reality (AR) technologies, featuring a mashup of massive multiplayer gaming, virtual worlds, virtual workspaces, and remote education to create a decentralized wonderland and collaborative space. The grand concept is that the metaverse will be the next iteration of the mobile internet and a major part of both digital and real life.

Don’t feel like going out tonight in the real world? Why not stay “in” and catch a show or meet people/avatars/smart bots in the metaverse?

As currently conceived, the metaverse, “Web 3.0,” would feature a synchronous environment giving users a seamless experience across different realms, even if such discrete areas of the virtual world are operated by different developers. It would boast its own economy where users and their avatars interact socially and use digital assets based in both virtual and actual reality, a place where commerce would presumably be heavily based in decentralized finance, DeFi. No single company or platform would operate the metaverse, but rather, it would be administered by many entities in a decentralized manner (presumably on some open source metaverse OS) and work across multiple computing platforms. At the outset, the metaverse would look like a virtual world featuring enhanced experiences interfaced via VR headsets, mobile devices, gaming consoles and haptic gear that makes you “feel” virtual things. Later, the contours of the metaverse would be shaped by user preferences, monetary opportunities and incremental innovations by developers building on what came before.

In short, the vision is that multiple companies, developers and creators will come together to create one metaverse (as opposed to proprietary, closed platforms) and have it evolve into an embodied mobile internet, one that is open and interoperable and would include many facets of life (i.e., work, social interactions, entertainment) in one hybrid space.

In order for the metaverse to become a reality – that is, successfully link current gaming and communications platforms with other new technologies into a massive new online destination – many obstacles will have to be overcome, even beyond the hardware, software and integration issues. The legal issues stand out, front and center. Indeed, the concept of the metaverse presents a law school final exam’s worth of legal questions to sort out. Meanwhile, we are still trying to resolve the myriad of legal issues presented by “Web 2.0,” the Internet we know it today. Adding the metaverse to the picture will certainly make things even more complicated.

At the heart of it is the question of what legal underpinnings we need for the metaverse infrastructure – an infrastructure that will allow disparate developers and studios, e-commerce marketplaces, platforms and service providers to all coexist within one virtual world. To make it even more interesting, it is envisioned to be an interoperable, seamless experience for shoppers, gamers, social media users or just curious internet-goers armed with wallets full of crypto to spend and virtual assets to flaunt. Currently, we have some well-established web platforms that are closed digital communities and some emerging ones that are open, each with varying business models that will have to be adapted, in some way, to the metaverse. Simply put, the greater the immersive experience and features and interactions, the more complex the related legal issues will be.

Contemplating the metaverse, these are just a few of the legal issues that come to mind:

- **Personal Data, Privacy and Cybersecurity** – Privacy and data security lawyers are already challenged with addressing the global concerns presented by varying international approaches to privacy and growing threats to data security. If the metaverse fulfills the hype and develops into a 3D web-based hub for our day-to-day lives, the volume of data that will be collected will be exponentially greater than the reams of data already collected, and the threats to that data will expand as well. Questions to consider will include:

- Data and privacy* – What’s collected? How sensitive is it? Who owns or controls it? The sharing of data will be the cornerstone of a seamless, interoperable environment where users and their digital personas and assets will be usable and tradeable across the different arenas of the metaverse. How will the collection, sharing and use of such data be regulated? What laws will govern the collection of data across the metaverse? The laws of a particular state? Applicable federal privacy laws? The GDPR or other international regulations? Will there be a single overarching “privacy policy” governing the metaverse under a user and merchant agreement, or will there be varying policies depending on which realm of the metaverse you are in? Could some developers create a more “privacy-focused” experience or would the personal data of avatars necessarily flow freely in every realm? How will children’s privacy be handled and will there be “roped off,” adults-only spaces that require further authentication to enter? Will the concepts that we talk about today – “personal information” or “personally identifiable information” – carry over to a world where the scope of available information expands exponentially as activities are tracked across the metaverse?
- Cybersecurity*: How will cybersecurity be managed in the metaverse? What requirements will apply with respect to keeping data secure? How will regulation or site policies evolve to address deep fakes, avatar impersonation, trolling, stolen biometric data, digital wallet hacks and all of the other cyberthreats that we already face today and are likely to be exacerbated in the metaverse? What laws will apply and how will the various players collaborate in addressing this issue?
- Technology Infrastructure**: The metaverse will be a robust computing-intensive experience, highlighting the importance of strong contractual agreements concerning cloud computing, IoT, web hosting, and APIs, as well as software licenses and hardware agreements, and technology service agreements with developers, providers and platform operators involved in the metaverse stack. Performance commitments and service levels will take on heightened importance in light of the real-time interactions that users will expect. What is a meaningful remedy for a service level failure when the metaverse (or a part of the metaverse) freezes? A credit or other traditional remedy? Lawyers and technologists will have to think creatively to find appropriate and practical approaches to this issue. And while SaaS and other “as a service” arrangements will grow in importance, perhaps the entire process will spawn MaaS, or “Metaverse as a Service.”
- Open Source** – Open source, already ubiquitous, promises to play a huge role in metaverse development by allowing developers to improve on what has come before. Whether or not the obligations of common open source licenses will be

triggered will depend on the technical details of implementation. It is also possible that new open source licenses will be created to contemplate development for the metaverse.

- **Quantum Computing** – Quantum computing has dramatically increased the capabilities of computers and is likely to continue to do over the coming years. It will certainly be one of the technologies deployed to provide the computing speed to allow the metaverse to function. However, with the awesome power of quantum computing comes threats to certain legacy protections we use today. Passwords and traditional security protocols may be meaningless (requiring the development of [post-quantum cryptography that is secure against both quantum and traditional computers](#)). With raw, unchecked quantum computing power, the metaverse may be subject to manipulation and misuse. Regulation of quantum computing, as applied to the metaverse and elsewhere, may be needed.
- **Antitrust:** Collaboration is a key to the success of the metaverse, as it is, by definition, a multi-tenant environment. Of course collaboration amongst competitors may invoke antitrust concerns. Also, to the extent that larger technology companies may be perceived as leveraging their position to assert unfair control in any virtual world, there may be additional concerns.
- **Intellectual Property Issues:** A host of IP issues will certainly arise, including infringement, licensing (and breaches thereof), IP protection and anti-piracy efforts, patent issues, joint ownership concerns, safe harbors, potential formation of patent cross-licensing organizations (which also may invoke antitrust concerns), trademark and advertising issues, and entertaining new brand licensing opportunities. The scope of content and technology licenses will have to be delicately negotiated with forethought to the potential breadth of the metaverse (e.g., it's easy to limit a licensee's rights based on territory, for example, but what about for a virtual world with no borders or some borders that haven't been drawn yet?). Rightsholders must also determine their particular tolerance level for unauthorized digital goods or creations. One can envision a need for a DMCA-like safe harbor and takedown process for the metaverse. Also, akin to the litigation that sprouted from the use of athletes' or celebrities' likenesses (and their tattoos) in videogames, it's likely that IP issues and rights of publicity disputes will go way up as people's virtual avatars take on commercial value in ways that their real human selves never did.
- **Content Moderation.** Section 230 of the Communications Decency Act (CDA) has been the target of bipartisan criticism for several years now, yet it remains in effect despite its application in some distasteful ways. How will the CDA be applied to the metaverse, where the exchange of third party content is likely to be even more robust than what we see today on social media? How will "bad actors" be treated, and what does an account termination look like in the metaverse? Much like the

legal issues surrounding offensive content present on today's social media platforms, and barring a change in the law, [the same kinds of issues surrounding user-generated content will persist and the same defenses under Section 230 of the Communications Decency Act will be raised.](#)

- **Blockchain, DAOs, Smart Contract and Digital Assets:** Since the metaverse is planned as a single forum with disparate operators and users, the use of a blockchain (or blockchains) would seem to be one solution to act as a trusted, immutable ledger of virtual goods, in-world currencies and identity authentication, particularly when interactions may be somewhat anonymous or between individuals who may or may not trust each other and in the absence of a centralized clearinghouse or administrator for transactions. The use of smart contracts may be pervasive in the metaverse. Investors or developers may also decide that DAOs (decentralized autonomous organizations) can be useful to crowdsource and fund opportunities within that environment as well. Overall, a decentralized metaverse with its own discrete economy would feature the creation, sale and holding of sovereign digital assets (and their free use, display and exchange using blockchain-based payment networks within the metaverse). This would presumably give NFTs a role beyond mere digital collectibles and investment opportunities as well as a role for other forms of digital currency (e.g., cryptocurrency, utility tokens, stablecoins, e-money, virtual "in game" money as found in some videogames, or a system of micropayments for virtual goods, services or experiences). How else will our avatars be able to build a new virtual wardrobe for what is to come?

With this shift to blockchain-based economic structures comes the potential regulatory issues behind digital currencies. How will securities laws view digital assets that retain and form value in the metaverse? Also, as in life today, visitors to the metaverse must be wary of digital currency schemes and meme coin scams, with regulators not too far behind policing the fraudsters and unlawful actors that will seek opportunities in the metaverse. While regulators and lawmakers are struggling to keep up with the current crop of issues, and despite any progress they may make in that regard, many open issues will remain and new issues will be of concern as digital tokens and currency (and the contracts underlying them) take on new relevance in a virtual world.

Big ideas are always exciting. Watching the metaverse come together is no different, particularly as it all is happening alongside additional innovations surrounding the web, blockchain and cryptocurrency (and, more than likely, updated laws and regulations). However, it's still early. And we'll have to see if the current vision of the metaverse will translate into long-term, concrete commercial and civic-minded opportunities for businesses, service providers, developers and individual artists and creators. Ultimately, these parties will need to sort through many legal issues, both novel and commonplace, before creating and participating in a new virtual world concept that goes beyond the massive multi-user videogame platforms and virtual worlds we have today.

[View Original](#)

[Related Professionals](#)

- **Jeffrey D. Neuburger**
Partner