



FAR FROM THE WILD WEST

Dr Mark Watts of Bristows LLP discusses how law and regulation may play a role in the metaverse fulfilling its potential.

The metaverse, which is for many the next great economic opportunity and successor to the internet, is attracting a lot of attention, investment and commercial interest (see box “What is the metaverse?”). Recent research suggests that the market opportunity may be worth over \$1 trillion in annual revenue (https://grayscale.com/wp-content/uploads/2021/11/Grayscale_Metaverse_Report_Nov2021.pdf).

It was a common myth during the advent of the internet that cyberspace was an unregulated place where no laws applied. One sometimes hears this of the metaverse too, although, as with the web, nothing could be further from the truth. While it is true that there is uncertainty regarding how some laws and regulations may apply in the metaverse, the fact remains that there is no shortage of existing laws and regulations. Indeed, multiple laws from many jurisdictions apply simultaneously.

This article discusses how law and regulation may play a role in the metaverse fulfilling its potential (see box “The metaverse of the future”). It examines the legal issues that are most relevant to the metaverse, in particular:

- Non-fungible tokens (NFTs).
- Trade marks.
- Copyright.
- Advertising.
- Financial services.
- Taxation.
- Data protection and privacy.
- Competition.
- Jurisdiction.

- Defamation.
- Online harms.

NON-FUNGIBLE TOKENS

NFTs provide the metaverse with a means of creating digital scarcity in respect of virtual assets that could otherwise be freely copied and therefore have no value (see *Exclusively online article “Non-fungible tokens: the new frontier of fraud?”*, www.practicallaw.com/w-032-6678). Already, they are big business. In March 2021, the digital artist known as Beeple sold an NFT of his piece “Everydays: The First 5000 Days” for an astonishing \$69 million (www.bbc.co.uk/news/technology-56362174).

Whereas a £10 note is fungible, that is, it can be traded for another £10 note, non-fungible items are unique and cannot be traded in the same way. Original artworks, limited edition

What is the metaverse?

At its simplest, a metaverse is an immersive digital world where users can live, socialise, work and play. Metaverses tend to be persistent; that is, “life” in the metaverse carries on even when a user is not present. As for what they look like, metaverses take many forms, usually involving some form of extended-reality (XR) technology, whether altering reality by adding digital elements to the real world, which is known as augmented reality or by creating a fully-immersive, 3D virtual environment that is explored by a user’s avatar, which is known as “virtual reality” (VR).

Although VR is not an essential aspect of a metaverse, most people tend to think of VR that requires a headset, such as a Meta Quest 2 or a PlayStation VR2, as the metaverse of the future. Many games already incorporate XR elements, the most famous example being the global phenomenon, Pokémon Go, where digital images of Pokémon characters are layered on real-world locations for players to interact with on their phones.

trading cards and private property are all non-fungible. In the same way that lottery tickets and shares in a company are tokens that represent something else, that is, entry into a lottery or ownership of part of a company, an NFT is a token that represents a record of ownership of a unique digital asset, such as a jpeg or gif image, or an audio or video file. It can be thought of as a digital certificate of authenticity. Stored and authenticated on a blockchain, usually the Ethereum platform, an NFT is nigh on impossible to tamper with because each of the nodes in the blockchain retains a complete copy of the ledger, confirming ownership (see *Briefing “Blockchain technology: emerging from the shadows”*, www.practicallaw.com/4-634-8506).

The rights attached to ownership of NFTs can vary from a simple, non-exclusive, non-commercial licence to display the asset publicly to additional rights to physical goods and services in the real world. A key benefit for artists and content creators who mint NFTs is the ability to attach a smart contract, which is essentially computer code, to facilitate, verify and negotiate an agreement between parties automatically and update the blockchain accordingly, making the transaction immutable.

One attraction of the metaverse is the degree of customisation and personalisation that users can apply to their digital identity; for example, by buying distinctive items of clothing for their avatar, hanging unique artwork in their digital homes or personal meeting spaces, or buying digital accessories for when they interact with other users, which could range from a designer handbag to a

bejewelled sword. Many users are likely to choose recognisable, real-life premium brands, a fact which is not lost on brands such as Gucci and Burberry, each of which has already offered NFTs of their products for sale. In addition, in December 2021, sportswear giant, Nike, took the bold step of buying virtual shoe company RTFKT, which makes NFTs and trainers for the metaverse (<https://about.nike.com/en/newsroom/releases/nike-acquires-rtfkt>).

One familiar problem that metaverse users may face is the difficulty in ensuring that they buy from NFT sellers offering authentic original art. Highly respected glitch artist Rosa Menkman publicly complained about this problem after finding five of her pieces advertised and sold as NFTs on the OpenSea platform without her authorisation. While NFT marketplace platforms can delist NFTs of plagiarised works, this will be of little consolation to buyers who spend their cryptocurrency only to find that it is the equivalent of a forgery. Buyers need to carry out thorough due diligence on NFT sellers and not rely on the platform to do this for them. OpenSea’s terms and conditions make this clear, stating that: “you bear responsibility for verifying the legitimacy, authenticity, and legality of NFTs that you purchase from third-party sellers” (section 5, *OpenSea terms of service*, 31 December 2021).

Although the English courts have gone some way toward recognising NFTs as property, such as in *Osbourne v Persons Unknown and Ozone*, metaverse users who suffer a loss when dealing in NFTs are likely to find themselves faced with another problem; that is, identifying who to sue ([2022] EWHC 1021).

Unlike an auction of traditional artwork at Sotheby’s or Christie’s, where the buyer or seller can be identified relatively easily, the anonymity provided by digital wallets in blockchain transactions can make it difficult for aggrieved parties to a transaction to initiate a claim (see *feature articles “International asset recovery: enforcement strategies”*, www.practicallaw.com/6-557-2166 and *“Tracing cryptocurrency: the challenges of Bitcoin”*, www.practicallaw.com/w-031-4385).

TRADE MARKS

While many well-known brands seem to be embracing the metaverse as a means of promotion, especially through NFTs, legal challenges remain. For example, trade mark infringement typically requires the use of a sign in the “course of trade” (section 10, *Trade Marks Act 1994*). If a user mints an NFT of a pair of Nike trainers for their avatar to wear, this use is arguably not in the course of trade.

Also, infringement of a UK trade mark requires use in the UK and, likewise, infringement in the EU requires use within the EU. This raises the issue of how this territorial nature might operate in borderless virtual worlds. The established “targeting” principles to determine if online use is connected are derived from a number of cases concerning traditional e-commerce platforms and focus on factors such as which top-level country domain, currency and language are used. However, with some metaverses, such as Decentraland, which operates a browser-based platform using a .org domain that allows users to trade virtual land using cryptocurrency, it is difficult to see a connection to any particular market.

Another question is whether an existing trade mark registration for real-world goods and services will afford protection in a virtual context; for example, whether a registration for trainers will cover virtual trainers. Brand owners should consider obtaining additional rights specifically for the virtual environment. There is also a question of whether a brand can leverage its real-world reputation to claim a reputation or goodwill regarding virtual goods; for example, whether Nike can claim a reputation or goodwill for virtual trainers based on the use of its marks in connection with physical trainers.

Brands such as Nike and Hermès have already taken legal action against digital content creators in the US. However, the greater

The metaverse of the future

Today, there is no single metaverse but separate ones that are provided by various platforms, making it more accurate to talk about metaverses than the metaverse. For some, however, the ultimate vision is of a single unified space, perhaps comprising multiple metaverses, but with sufficient interoperability for users to move seamlessly from one to another, for example from a Meta one to a Microsoft one. Unfortunately, there is currently little interoperability, and moving from one metaverse to another usually requires a change of headsets, logging into a different account and using a different avatar.

Estimates of how long it may take to develop the technology necessary to realise this single joined-up metaverse vision vary but, for most, it is several years, and there are substantial commercial challenges too. True interoperability requires close co-operation between competitors and for the digital assets acquired by a user in one metaverse to be recognised in another. A fully immersive, interoperable metaverse experience does not feel imminent, but technology has a habit of proving naysayers wrong. Ten years ago, few would have predicted that people would spend so much of their time looking at mobile screens, yet that is now the current position.

Some regard success simply as the metaverse becoming more than a gaming platform and providing a means of performing other aspects of human life (see box “*Gaming in the metaverse*”). They point to examples of online games that have become social networks and, in some cases, such as Discord, platforms for education and work as well. Others, however, such as Meta’s CEO Mark Zuckerberg, go further. His vision is of a 3D version of the internet that “delivers a deep feeling of presence”, achieving a level of immersion that mimics the real world through the degree to which the technology can give virtual environments sights, smells and sounds.

However, the level of immersion and how closely it replicates real life is surely only one aspect. It seems likely that there also needs to be some enhancement or benefit over real life for people to be willing to wear a virtual reality headset and a haptic suit, which replicates aspects of the sense of touch, for any prolonged period. For many, the paraphernalia necessary to access a 3D virtual world presents a significant obstacle, at least at the moment. So it is fair to say that an entirely virtual life is not likely to replace real life anytime soon. Still, it is probably also true that there will soon be many situations, such as digital art galleries and international business meetings, where the new possibilities that a metaverse offers sufficiently outweigh any inconvenience of getting there in person.

in the metaverse. The product placement that is common in TV shows and movies could become a part of our everyday lives. An example of the type of question that could arise is whether it is advertising if a beer brand pays a provider to have virtual bottles on the tables of a virtual pub. If the metaverse is treated like a website and the appearance of the bottles is the equivalent of online display advertising, the answer is probably yes. If, however, the appearance of the bottles is treated in the same way as distributing free product samples, the answer may be no. Advertising regulators will need to decide questions such as whether metaverse users should have the right to know that these virtual bottles are present in the virtual bar because the beer brand paid the provider of the environment.

Where a metaverse product is bought using a virtual currency that can only be earned through activity in that metaverse, it seems unlikely that real-world regulators would take an interest in its advertising. However, the situation may be different if users can also acquire the virtual currency using Bitcoin or US dollars, giving it value in real-life currency. In these circumstances, advertising for products bought using virtual currency may be of more interest to real-world regulators.

Age restrictions also need to be considered. In the UK, for example, no advertising medium may be used for alcohol adverts if more than 25% of its audience is under 18 years of age. It seems likely that age assurance to ensure that users are above a certain age will also have a greater role in the metaverse.

COPYRIGHT

With copyright aiming to encourage and reward creativity, and with the metaverse, as many claim, providing greater opportunities for creativity, the two seem well-aligned in their objectives on the face of it. For example, users may be able to create artistic works that are physically impossible in the real world, such as Meta’s Horizon Home, where users will be able to create their own houses, unconstrained by the physics of the real world, and claim copyright in them as original artistic works.

Overall, the copyright position will likely depend on whether the metaverse is “open” or “closed”. In an open metaverse, such as Decentraland, there is no central authority, and the rights remain with the users; these

anonymity of avatars may make it challenging to identify infringers, and the use of NFTs may make it harder for brands to connect the owner of an NFT to a real-world person. An alternative to legal action might be to consider a commercial approach such as collaborating or using cross-promotional branding to reach new audiences. For example, if a digital artist were to develop a hugely popular range of unauthorised branded NFTs, there might be more to gain for that brand owner by harnessing user engagement, perhaps by verifying or authorising certain NFTs or digital assets, rather than by using traditional enforcement methods. Brands will need to develop a strategy on what types of use to oppose, which uses can be tolerated and which ones can be commercialised.

ADVERTISING

The metaverse presents a significant advertising opportunity, increasing the number of goods and services that can be advertised to include real-world goods and services and their virtual equivalents (see feature article “*The adtech challenge: thriving in an e-commerce world*”, www.practicallaw.com/w-032-9223). The highly immersive nature of the environment and the opportunity to target users are also attractive to advertisers.

Regulators have grappled with the issue of native advertising, that is, advertising that blends into its surroundings, for many years, and this issue will be particularly significant

platforms would likely merely require a licence to the platform or the community to use user-created elements. In a closed metaverse, users may not be able to build on the code of the metaverse in question and may only be able to create works, such as virtual houses, according to the platform's functionality. Being centralised, the operator in question in a closed metaverse may also have a greater say regarding copyright ownership through its terms of service.

While the question of infringement will essentially operate as it does now, as with trade marks, its detection may present a new challenge. For example, typical search functions may fail to identify infringing code contained within a blockchain. Furthermore, current open metaverse platforms such as Decentraland and The Sandbox may not be easily searched for infringements; finding infringements could require virtual exploration and perhaps new detection technologies will need to develop.

There is no point in owning copyright if the owner cannot enforce it, so platforms will also need to consider how to deal with this. But, again, the open or closed nature of the metaverse in question will be relevant. Closed, centralised platforms are the most likely to adopt a light monitoring procedure, filtering out the most obvious infringements primarily using technology, perhaps supported by a notice-and-takedown procedure. An open, decentralised metaverse, however, raises several enforcement issues. Asserting copyright in a notice-and-takedown style may be difficult without a central authority.

FINANCIAL SERVICES

Currently, there is a particular regulatory focus on two critical components of the metaverse: digital currencies and NFTs. Both of these rely on blockchain technology without the need for a financial intermediary, such as a bank. Given that it is intermediaries that enforce financial regulatory checks and have obligations to prevent money laundering, terrorist financing and other forms of financial crime, the metaverse poses a particular challenge for financial services regulation.

A key challenge in regulating digital currencies is the speed and ingenuity with which new ones are developed. It is an ever-changing landscape, from cryptocurrencies, such as Bitcoin, to lesser-known stablecoins, such as Tether, which are tied to fiat currencies

Gaming in the metaverse

Many of the metaverse's building blocks have been around for years, particularly in gaming, as has the idea of blurring the line between real and virtual life. This was present in Linden Labs' 3D virtual world, Second Life, in 2003, which still has an active community of users using avatars to live in a 2D digital world and is regarded by its users less as a game than a place to spend time, with amenities such as universities, nightclubs and churches.

Other games to offer an immersive environment include Minecraft and Roblox. Roblox, in particular, is avatar-led, with an active marketplace for digital assets, such as new costumes, pets and houses to improve the avatar's life. Fortnite, which started as a battle royale game, has expanded recently into a pop culture platform, hosting live music concerts. Meta's Horizon Worlds consists of a virtual reality (VR) social networking and gaming platform with a central street, the Plaza, from which users can access various gaming and creative worlds.

Other technology companies are also investing heavily in metaverse offerings. For example, Microsoft announced plans to launch its metaverse platform, Mesh, in 2021. Microsoft, which owns World of Warcraft and Minecraft, may bring a different aspect to its metaverse, combining its vast experience in enterprise software with expertise in gaming. Perhaps unsurprisingly, its first Mesh product is a VR add-on to Teams, a business communication tool.

Not all metaverses are provided by big technology companies. Decentraland and The Sandbox use blockchain technology to create virtual worlds where users can buy various parcels of non-fungible tokens, known as LAND, using cryptocurrency. Both claim to be decentralised and owned by their users. Decentraland allows users to vote on strategic matters based on the LAND and in-game cryptocurrency that they own, which is an example of a decentralised autonomous organisation.

like the dollar (see *Briefing "Stablecoins and central bank digital currencies: a developing landscape"*, www.practicallaw.com/w-028-0710).

In the UK, some are regulated by the Financial Conduct Authority (FCA), while others are not. Similarly, the European Commission's (the Commission) draft regulation on markets in cryptoassets, which is due to be implemented in 2024, aims to define the regulatory treatment of all cryptoassets that are not covered by existing financial services regulation and instil appropriate levels of consumer and investor protection ([https://ec.europa.eu/transparency/documents-register/detail?ref=COM\(2020\)593&lang=en](https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2020)593&lang=en)).

The regulation of the NFT market is even less clear, with NFTs not falling directly within the remit of either the FCA's or the Commission's approach to cryptoassets. The Financial Action Task Force (FATF), an intergovernmental body that sets international standards for the prevention of money laundering and terrorist financing globally, recognises the need for clarification

(www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf). It recommends that certain NFTs should be categorised as virtual assets (VA) and regulated accordingly. It states that "some NFTs that on their face do not appear to constitute VAs may fall under the VA definition if they are to be used for payment or investment purposes in practice" and it recommends that countries should therefore consider the application of the FATF Standards to NFTs on a case-by-case basis.

If an NFT fits the definition of a VA, the service providers involved could fall within the meaning of a VA service provider and become financially regulated entities with obligations including "know your client" checks, robust verifications for the products being sold, record-keeping, and other anti-money laundering requirements.

The prevalence of fraud in the NFT market, such as tokenisation, wash trading, insider trading and sleep minting, heightens the pressure to create a regulatory framework, even where an NFT is not considered to be a

VA. Governments have also become aware of the increasing risk of tax evasion when NFTs and cryptoassets provide anonymity as their ownership is not linked to a legal person but only to a digital wallet. Given the sums involved, with the NFT market surpassing \$40 billion in 2021, financial regulators are unlikely to leave this area untouched for much longer (see feature article "FCA and PRA enforcement actions: trends and predictions", www.practicallaw.com/w-034-1498 and News brief "Cryptoasset promotion: clamping down on marketing high-risk products", www.practicallaw.com/w-034-5146).

TAXATION

According to Benjamin Franklin, death and taxes are the only two certainties in life. Is this also true of life in the metaverse? With death, who knows (perhaps an avatar will eventually be able to live beyond the life of its user)? In the case of taxes, however, the position is slightly clearer. Transactions in the virtual world will still generate value for real-world persons connected to them, so existing international tax rules will apply. Nevertheless, there may be challenges and some uncertainty.

In many cases, identifying that a transaction has occurred will be straightforward. The online purchase in the metaverse of real-world goods or services will likely follow established rules that apply to online transactions. However, where the transaction is the exchange of one virtual asset for another, such as an NFT acquired with cryptocurrency, it may be less obvious how the rules apply.

The UK's position on the direct tax treatment is relatively clear. Applying these principles to a hypothetical transaction where a UK consumer uses cryptocurrency to acquire a limited edition NFT accessory from the metaverse store of a UK company, the following tax liabilities could arise:

- Capital gains tax (CGT) for the individual on the disposal of their cryptocurrency when buying the NFT, assuming that the value of the cryptocurrency has increased.
- Corporation tax for the UK corporate on the profit generated from the sale of the NFT.
- CGT for the individual on any future sale of the NFT, again assuming that its value has increased.

The indirect tax treatment, that is, the sales tax or VAT position, is less clear. Spain is the only European jurisdiction at the moment with a clear tax ruling specifying that NFTs attract VAT. The question of which tax authority has jurisdiction can also be unclear. Current tax rules require the tax residency of the real-world parties to the transaction to be determined, but questions arise as to how these rules apply to a metaverse sale by a decentralised, member-owned and controlled organisation governed by blockchain-powered smart contracts.

Regarding tax collection, the starting point has to be reporting, and the Organisation for Economic Co-operation and Development is consulting on a framework for the automatic exchange of information on cryptoassets, which was published in March 2022 (www.oecd.org/tax/exchange-of-tax-information/public-consultation-document-crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.pdf). These proposals require a cryptoasset service provider to provide identifying information on its users and a list of cryptoasset transactions. This framework may need to be extended to capture metaverse platform hosts. In much the same way that online sales platforms have been forced to act as VAT collectors in respect of transactions facilitated by their platforms, metaverse providers may need to accept a degree of responsibility for policing tax in the worlds that they have created.

DATA PROTECTION AND PRIVACY

The General Data Protection Regulation (679/2016/EU) (GDPR) (or the version retained in UK law, the UK GDPR) will apply to metaverses that are controlled or processed by providers established in the UK or EU. Even for providers outside of the UK and EU, the GDPR is likely to apply if they are targeting or monitoring the behaviour of individuals in the UK or EU. The consequences of this are too many and profound to set out in full here, being backed up by eye-watering fines of up to 4% of global turnover (see feature article "GDPR enforcement: a changed landscape", www.practicallaw.com/w-030-5470).

The EU's draft e-Privacy Regulation, which will regulate the setting of cookies and processing of user data for online advertising purposes, will also have a significant impact (see News brief "Latest e-Privacy Regulation proposals: breaking the deadlock?", www.practicallaw.com/w-024-5857).

Between them, the GDPR and the e-Privacy Regulation will determine what data about a user's interactions in the metaverse, with the platform, any secondary marketplace and with other users, may be used to generate advertising revenue to fund what may be a free service. This is not a new issue, although the greater volume and richness of user data in an environment where everything exists only virtually promises to make it even more significant.

Other current and proposed EU laws, such as the Data Act, the Data Governance Act and the Digital Services Act, may also have an impact on the development of the metaverse, affecting the data sharing between providers, that is necessary to realise the vision of a single metaverse, and online advertising (see feature articles "Regulating digital services in the EU: a paradigm-shifting legislative framework", www.practicallaw.com/w-030-6172 and "EU regulatory data framework: a new generation", www.practicallaw.com/w-036-5428).

The additional requirements for processing special category data will also be relevant. Offline, there could be a greater collection of biometric data, such as virtual reality (VR) headsets that collect data about a user's pupil dilation. At the same time, in the metaverse, there are difficult questions regarding an avatar's status, particularly a highly realistic one; for example, whether a user's choice of particular attributes, such as race and ethnicity, could result in a metaverse provider processing special category data. The context is likely to be key because in the gaming environment an avatar often need not bear any resemblance to the user in the real world.

Other privacy rights, such as those in Article 8 of the European Convention of Human Rights, will also be relevant, where, for example, a user is wearing a VR headset in a private space, such as their bedroom, and cameras and other sensors on the device are collecting private information, irrespective of whether that data is personal data.

COMPETITION

Competition laws apply to companies operating in the metaverse; indeed, those involved in research and development for the metaverse should already be addressing competition law issues in their licence agreements. However, other issues are also likely to arise.

Should a company manage to create a single metaverse used by the vast majority of users, it may hold a dominant position and so be under a special responsibility not to abuse its market power. For example, it could be unlawful for the dominant company to refuse to allow other businesses to participate in the metaverse economy, to refuse access to data or to favour its own products and services. A dominant company would also have to consider how its conduct affects any secondary marketplaces that may develop. For example, the Commission and the Competition and Markets Authority are investigating Amazon Marketplace to assess whether Amazon is giving an unfair advantage to its own business or sellers that use its fulfilment services (https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077; www.gov.uk/government/news/cma-investigates-amazon-over-suspected-anti-competitive-practices). Similar issues could arise in a marketplace for virtual assets.

What seems more likely, however, is that several metaverses will evolve, as is the case at the moment. One of the most interesting questions is whether it will be possible to move seamlessly between metaverses; for example, where a user could use their avatar to attend a work meeting in the Microsoft metaverse, followed by meeting friends in the Meta metaverse (see box “*The metaverse of the future*”). Users would also want to be able to use any digital products that they buy across all metaverses. This is already happening with current gaming platforms, leading to Fortnite skins and V-bucks in-game currency now being available across platforms.

However, creating this kind of seamless movement between metaverses would require tremendous interoperability, that is, common technical and data standards, to enable real-time exchanges of information. The companies would also need to share commercially sensitive information about how their metaverses operate and how they may do so in the future. Sharing technical information can be pro-competitive and benefit consumers. For example, in the context of mobile phones, it would be frustrating if a user on the Vodafone network could not communicate with a user on the EE network. As a result, companies involved in the mobile ecosystem, from network infrastructure to chipsets to handsets, have worked together to create standards to enable interoperability and solve these issues.

However, sharing this information can potentially be highly anti-competitive. To avoid anti-competitive effects, metaverse companies would need to show that end consumers benefit from interoperability and that they are not exchanging more information than is necessary to create the required technical standards or using it to preclude competition. Some metaverse companies may resist standardisation, preferring to try and lock in users to their system by making it the preferred choice of as many users as possible.

Intellectual property rights are likely to be highly relevant to any metaverse standards that are created. For example, in the mobile phone context, thousands of patents are essential to the 4G and 5G standards, any one of which could potentially be used to obtain an injunction to block sales of a phone that complies with the standard. As a result, patentees must license these standard essential patents on FRAND (fair, reasonable and non-discriminatory) terms to ensure that they cannot take advantage of the standardisation process. Metaverse companies involved in creating common standards may need to adopt a similar approach.

JURISDICTION

Issues of jurisdiction will arise in the metaverse. These can be illustrated by a hypothetical situation of a person attending a concert in the metaverse from their home in the UK, where the metaverse is hosted on a South Korean server. If the artist sings from their home in the US, and a concert promoter sells the tickets in Canada, issues to consider include where the concert is taking place and which court or courts have jurisdiction. It sounds like an exam question, but it is a question that lawyers will increasingly have to grapple with.

Typically, countries have rules to assist their courts in determining whether they may exercise jurisdiction over a dispute. These tend to be informed by principles found in the Charter of the United Nations, such as sovereign equality, non-intervention and territorial integrity. In addition, many countries are parties to international conventions regarding jurisdiction over cross-border disputes and, in some cases, the recognition and enforcement of judgments, such as the Hague Convention on the Recognition and Enforcement of Foreign Judgments in Civil

or Commercial Matters, which was adopted on 2 July 2019.

In response to the growth of the internet, countries have adapted their legal frameworks and created new laws to determine which courts have jurisdiction over disputes that arise online. However, consideration will need to be given as to whether those rules will need to change given the development of the metaverse and the avatars that inhabit it. Alternatively, the platforms might seek to impose their own dispute resolution mechanisms, in a similar way to eBay’s dispute resolution process for buyers and sellers.

DEFAMATION

A number of defamation-related issues could arise in the metaverse. These can be illustrated by a hypothetical situation of a person attending a conference in the metaverse, represented by their avatar, where an industry expert giving a presentation makes a false and defamatory remark, causing harm to that person’s reputation. They could bring a claim against the expert, but they would need to consider how the claim would be affected by the fact that it is the avatar that has been defamed, which may not bear any resemblance to the person in real life, may have a different identity and may have cultivated a reputation of its own running a successful metaverse business, such as a gallery selling NFTs.

A key requirement of a defamation claim is that the statement complained of identifies the claimant. This does not mean that the claimant has to be named; identification by reference to their business or address is sufficient. In the example of the gallery-owning avatar, the relevance of whether anyone knows the real-life identity of the person behind the avatar may need to be considered. If their NFT gallery is being affected financially and is owned by a limited company in the real world, one option could be for the company to bring a defamation claim, relying on a drop-off in custom to satisfy the necessary threshold of serious financial loss. Here, the court would need to be satisfied that a reference to the avatar would be understood as a reference to the company. If the allegation is personal to the avatar rather than specifically related to the gallery, this may be a non-starter. The answer might simply be that if no-one knows the person’s real-life identity, neither they nor their avatar can do anything about it.

Another unknown is whether what was said constitutes libel or slander. Libel is defamation in a permanent form, for example, when it is published in a newspaper or posted on social media, whereas slander is transitory, for example, using the spoken word or a gesture not in a permanent form. It matters because an action in slander is harder to establish, mainly because there are specific requirements relating to the damage that must have arisen due to what has been said.

In the example of a conference, if the conference took place in the real world and the speaker made a defamatory remark, this would likely constitute slander. In the metaverse, the position is not so clear and could, conceivably, vary from platform to platform, depending on the technology and functionality offered, as to how transitory the remarks really were.

ONLINE HARMS

There have already been reports of incidents of sexual assault on virtual reality games and platforms, underlining the need for metaverse platforms to take effective steps to minimise harms. For example, in Meta's Horizon, avatars can activate a safe zone to create a protective bubble around themselves where they cannot be touched, spoken to, or interacted with by other users. The question arises of whether user safety is the users' own responsibility or that of the platforms, or whether it should be a shared responsibility.

In the UK, the proposed Online Safety Bill (the Bill) would make it the platform's responsibility to proactively protect users (see *News brief "Online Safety Bill: do no harm?"*, www.practicallaw.com/w-035-3154). The Bill obliges platforms that allow users to share and encounter content from other users in the UK to conduct risk assessments of illegal content and remove the most heinous, such as terrorism or child sexual abuse material. There is also a duty to regulate and separately assess risk for legal but harmful content. In addition, platforms with the riskiest services to be categorised by the UK's newly designated body for online safety, Ofcom, must set out clearly and accessibly in their terms of service how different kinds of legal but harmful content available on their platforms will be treated; that is, whether it will be taken down, given less access or afforded less promotion.

By contrast, the EU approach in the proposed Digital Services Act is lighter, imposing a duty

Related information

This article is at practicallaw.com/w-036-5862

Other links from uk.practicallaw.com/

Topics

Advertising and marketing	topic/0-103-1114
Copyright	topic/0-103-1270
Data protection: general	topic/1-616-6550
E-commerce	topic/2-103-1274
Fintech	topic/w-012-0924
GDPR and data protection reform	topic/7-616-6199
General competition	topic/8-103-1167
Information technology	topic/5-103-2074
Internet	topic/8-383-8686
IP and IT: tax	topic/1-376-3552
Regulatory regime: financial services	topic/9-103-1355
Trade marks	topic/2-103-2080

Practice notes

Competition compliance toolkit	2-515-3708
Digital marketing: an overview	8-384-8223
Digital services tax	w-021-1734
FCA regulation of cryptoassets: overview	w-026-1787
FinTech: UK financial services regulatory overview	w-014-6806
Online platforms: dealings with consumers and business users	w-021-0867
Overview of copyright	9-107-3741
Overview of trade marks	4-107-3668
Overview of UK GDPR	w-013-3757
Taxation of cryptoassets	w-023-2579

Previous articles

FCA and PRA enforcement actions: trends and predictions (2022)	w-034-1498
GDPR enforcement: a changed landscape (2021)	w-030-5470
Regulating digital services in the EU: a paradigm-shifting legislative framework (2021)	w-030-6172
The adtech challenge: thriving in an e-commerce world (2021)	w-032-9223
Tracing cryptocurrency: the challenges of Bitcoin (2021)	w-031-4385
Challenges in the consumer sector: adapting to the new reality (2019)	w-020-8428
Challenges in the consumer sector: transformative technology (2019)	w-020-3706
Initial coin offerings: the good, the bad, and the ugly (2018)	w-013-2485
Blockchain and IP: crystal ball-gazing or real opportunity? (2017)	w-010-1622
International asset recovery: enforcement strategies (2014)	6-557-2166

For subscription enquiries to Practical Law web materials please call +44 0345 600 9355

on platforms to provide transparency reports on the actions taken to remove illegal content or legal content that contravenes their terms of service.

If the defining feature of the metaverse is a feeling of presence that goes beyond social media, regulators will need to rethink what harm might look like and how it should be handled. For example, they will need to consider what might constitute an assault in the metaverse. It may feel quite real for

a victim despite experiencing it through an avatar; however, several popular virtual games feature violence. Again, the context would appear to be important.

There is also a question over whether the embodiment of a user as an avatar will make a user more likely to behave in the metaverse because it feels closer to real life or more likely to misbehave because of the relative anonymity that an avatar can bring. Anonymity can be two-edged. On the one

hand, it may be life-enhancing, with the most vulnerable in society finding help or relief only through expressing a different persona in the virtual world, while on the other, it can give power to perpetrators of harm online through the ability to hide behind an avatar that does not resemble their true identity.

FUTURE REGULATION

The metaverse may already be one of the most regulated of spaces there is, with multiple laws from many countries all applying at the

same time, although in an uncertain way. As the metaverse grows, more laws may be needed in some areas and perhaps fewer laws in others, or perhaps just more metaverse-friendly interpretations from courts and regulators.

New laws may be needed to increase business and consumer confidence sufficiently for the metaverse to fulfil its ultimate potential. Equally, a knee-jerk or high-handed legislative approach could result in laws that stifle innovation and growth in a way that is

counterproductive. If new laws are needed, they need to be the right sort, striking the appropriate balance between the interests of all of the relevant stakeholders, which is a delicate balance indeed.

It has been said that it is possible to tell when a new technology has really arrived because the lawyers start talking about it. If this is true, then perhaps the metaverse is already here.

Dr Mark Watts is a partner at Bristows LLP.

Bristows Tech Summit...

Coming soon!

Save the date.

To hear more about the Metaverse and other exciting developments in the world of technology, **register your interest** for our upcoming tech summit taking place this year on **24 November**.