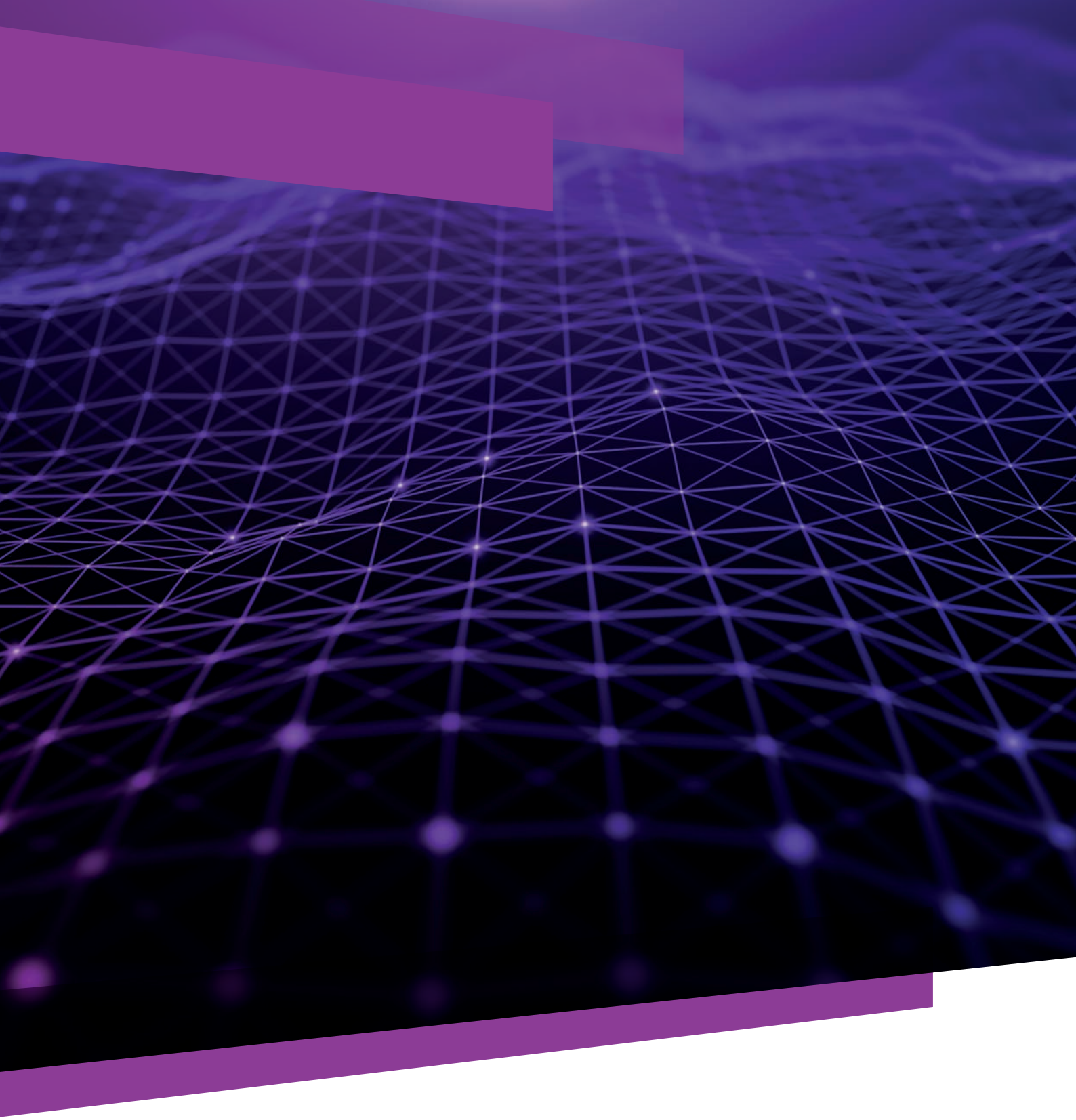


Reed Smith Guide to the **Metaverse** – 2nd edition

August 2022

ReedSmith

Driving progress
through partnership

Contents

The metaverse and what it means for business 03
What is the metaverse? 04
Glossary of terms 10

Entertainment and media in the metaverse 19
Advertising 20
Games: An NFT-powered revolution? 22
Games and metaverse issues 25
Music 28
Film and TV 36

Legal issues in the metaverse 39
Intellectual property 40
Investing in the metaverse 48
Artificial intelligence 52
Data protection and privacy 62
Content exploitation 70
NFTs: Ownership in the metaverse – the birth of a new concept 76
Is my NFT a security? 82
The ultimate NFT? 86
Investing in crypto 87
Crypto and other digital assets 88
Europe 89
United States 93
UAE 95
Deepfakes in the metaverse 98
Managing antitrust and competition risk 100
Aviation in the metaverse: Breaking the reality barrier 104
Insurance issues in the metaverse 108

The metaverse and what it means for business

By nature, lawyers are curious creatures, who are always eager to learn and react to new ways of doing things. The law is mostly precedential, built on a foundation of prior experience. It is the result of centuries of human transactions and behavior and the reactions and influence of governments and lawmakers. The concept of a virtual, alternative world – a metaverse – then, is naturally seductive to lawyers. It is a new world: an evolving, alternative digital environment in which change can happen in the blink of an eye. Driven by the dramatic evolutionary combination of technology, devices, and communication networks, the metaverse offers human beings the opportunity to collaborate, transact, perform, argue, and create as has never been seen before. Some would argue that it enables our alternative selves as humans.

Since the first edition of our *Guide to the Metaverse*, the use cases for the technologies that underpin these new online environments have developed significantly and, similarly, the regulations and body of law governing them have evolved. Given the rate of change in this area, deciphering the law pertaining to these virtual environments and being able to guide, advise, and support companies and individuals who operate in them requires both a strong handle on centuries of legal precedent and minds that are open to adapting and learning new legal skill sets. Since the first edition, we have been involved in advising on many cutting-edge applications of so-called web3 applications, including disputes and metaverse curiosities, and we have been helping companies develop their own virtual environments. We have also been interpreting laws that are not intended for virtual personalities, creating contracts pertaining to artificial intelligence applications that generate art and other products, and working with avatars that are loved by millions of real people.

Our team at Reed Smith enjoys the benefit of one of the longest histories of any law firm; we have been leading advisers in the media sector for more than 100 years. While we are never arrogant enough to think that we can enjoy another 100 years at the forefront, we are excited to engage with and advise our clients during what is undoubtedly the biggest industrial revolution the world has ever seen. The next advent of the metaverse and decentralized features of what is becoming known as Web 3.0 (or "web3," depending on whether you are a fan of Elon Musk or not) offers tremendous opportunities for growth and creativity. Although the entertainment and media sector is at the cutting edge of this phenomenon, the rest of the commercial world is close behind: health care, finance, energy, logistics, and even the more traditional manufacturing industries will soon be affected by what is happening in these new online environments. The consumer metaverse currently only affects a relatively small number of people; the enterprise metaverse will affect us all.

In this updated edition, we cover the key developments that have taken place in web3 in the last year, from the development of new regulations to real-world examples of the technologies in practice. We hope that this overview will be of use and practical application to those who are curious, as we are, about what the metaverse can become.

Gregor Pryor
Partner
London
gpryor@reedsmith.com

Stephen E. Sessa
Partner
Century City
ssessa@reedsmith.com

What is **the metaverse**?

The word itself means "beyond the universe," but what exactly is the metaverse? One way to describe it is the increasing permeability of the borders between different digital environments and the physical world. The metaverse is a space where you can interact with virtual objects in real life and with real-time information.

Adopting this literal approach to the metaverse means it is a combination of three elements. First, it is a technology that enables digital content to be laid over the real world. This is similar to augmented reality (AR). A simple example is the popular smartphone game, Pokémon Go, although, in the next iteration of a metaverse, this technology would be enhanced. Digital content is combined with the real world. Second, the metaverse applies a hardware device that enables the real world to be interactive. Digital content is applied so that users can control the content displayed virtually and interact with it within a real-life space. Third, it is information about anything and everything in the physical world (for instance, an area, a shop, or a product) and knowledge about the user (such as the user's schedule, location, habits, and interests). This information will be obtained from the internet and from machines learning about a user's everyday actions. A simple example of a device learning based on a user's everyday activities is Siri (on iOS) and Alexa (on Amazon). Real-time information is obtained instantly and virtually through the device into the physical space to optimize a user's experience, while in the background, data is collated and applied.

A less literal but no less relevant approach to understanding the metaverse is the application of real-world characteristics to a purely online environment. In the same way that digital content can be applied to the real world, a metaverse environment can apply real-world features to a virtual environment. For example, players interacting in a virtual gaming environment can walk around a virtual London or New York, seeing digital depictions of real-life streets and buildings. They can visit a virtual Apple store to browse and buy digital depictions of Apple products that can be delivered, in real life, to their actual physical homes. In many respects, this would be only an extension of what we know today as traditional e-commerce. However, as visual technology and design capability evolve, brands can create metaverse environments that not only replicate a real-life experience but improve it. There may be no line outside the virtual Manhattan Apple store when a new product is launched.

The idea of replicating real-life environments in the virtual world is not at all new. After all, Second Life still exists. However, modern-day gaming environments have moved the metaverse far beyond the clunky, socially awkward, and often avatar-limited 3D block worlds prevalent at the turn of the century into entirely new, ever-evolving creative online habitats. Virtual platforms like The Sandbox, Illuvium, or Decentraland, which offer innovative opportunities to build, create, trade, and explore while engaging with users from all around the world, have been at the forefront of the metaverse movement.

How does the metaverse work?

It is usually necessary to use a device to connect a user to the metaverse. This device might be a pair of goggles, a head-mounted apparatus with a camera feature, or a new invention we have yet to see. Such devices are not critical to engaging with the metaverse, but they can definitely amplify the experience. "Wearing" a device connects the user to the metaverse by integrating all of the elements and displaying the interactable virtual objects in real life. The interaction means that the user is able to react to the virtual objects; everything is displayed in real time, in front of them, in the physical world.

While such an advanced reality may be disconcerting, its fundamental elements are already widely adopted through mobile technology. Your smartphone knows you; it knows where you are and when. While the visual interfaces may change over time, the underlying capability needed to combine the physical and virtual worlds has existed for over a decade.

In the purely online world, the metaverse works by offering an escape from reality. However, there has been a significant shift in recent years toward the introduction of real-life elements into this escapist paradigm. Want to watch a movie within Roblox? Want to buy some sneakers while playing Grand Theft Auto? Want to see the latest live performance by a K-pop band on TikTok? It is this migration of commerce and interaction online and into virtual environments, and the increasing confluence between virtual and physical worlds, that drives the metaverse.

What are the commercial applications of the metaverse, and who will benefit from it?

The metaverse will alter the way we act, socialize, work, and live our lives. Just some of the potential commercial applications are discussed here, but there are business opportunities for participants in every sector, from consumer-driven industries, such as retail and events, to manufacturing, construction, and beyond.

The impressive opportunities and capabilities of the new technologies attract both consumers and tech giants, such as Roblox, Microsoft, and Nvidia. Meta (formerly Facebook) has also embraced virtual reality (VR) and augmented reality (AR) to create its own digital space, the so-called "metaverse," where people can get together, learn, work, play games, shop, and even do business in a virtual environment. Following the pioneering introduction of its AR glasses nearly a decade ago, Google has also been investing heavily in metaverse projects. The investment made by such businesses is no surprise when it has been estimated by PwC that VR and AR could deliver a $1.5 trillion boost to the global economy by 2030.

We have also seen a range of music businesses seeking to make their mark in the metaverse. Leading the way in innovation among major labels is Universal Music Group with its web3 label "10:22PM," which formed the metaverse boyband Kingship, comprised of "Bored Ape Yacht Club" NFT characters. In a similar vein, Warner Music Group has partnered with The Sandbox to create a music-themed world, called WMG LAND, within the gaming platform. And let's not forget the inimitable FN Meka, created by Anthony Martini and Factory New. FN Meka is a virtual rapper and influencer with more than 10 million TikTok followers.

On the consumer side, there is a growing appetite to shop online while socializing, which may prompt major retailers to enter the metaverse. In March 2022, we even saw the first Metaverse Fashion Week, which was hosted in Decentraland. Avatars will also be an important element of the metaverse experience, as they will express users' identities and represent who they are in the virtual world.

The increased connectivity provided by the metaverse means that goods will be more accessible, and businesses will be able to sell their goods worldwide regardless of the geographic location of their stores. User engagement will also be higher, which is likely to have a positive commercial impact if used properly.

Businesses can already sell VR accessories and services in the metaverse, much as they can in everyday life. NFTs and cryptocurrencies have been at the center of metaverse technology, enabling users to trade and invest. Users are now able to purchase anything from a digital artwork NFT to a parcel of land or real estate in the metaverse.

The metaverse has also had a huge impact on revolutionizing gaming and the way we socialize through games. For example, fans from across the globe are now able to participate in e-sports and gaming tournaments, like the EA Sports FIFA 22 Champions Cup.

Ultimately, consumers will gain most from the metaverse as information, products, entertainment, and social experiences are enhanced and more accessible.

Hardware technology companies and software development companies will dominate the technology market. The demand to provide hardware and software for the metaverse will drastically increase. Businesses will have the opportunity to create their own place in the metaverse. Brands and celebrities will have more exposure to wider audiences. The capability to offer richer, more targeted commercial promotions and experiences to consumers will increase.

And finally, how could we forget that there will also be a need for legal advice due to the uncertainty of the law and regulations around the metaverse? As we write, there is huge demand for advice in areas such as data protection, privacy, and advertising regulations – to ensure that commercial enterprise intellectual property assets are protected as the virtual and real worlds converge. Businesses will be keen to understand both the opportunities and the risks posed by the metaverse and to avoid the costly mistakes made by others, such as Spice DAO, a decentralized autonomous organization (DAO) that won an auction at $3 million to buy a manuscript of Alejandro Jodorowsky's failed adaptation of Frank Herbert's novel "Dune." The DAO had plans to digitize and sell the book as NFTs, as well as other derivative projects, before being confronted with the reality that it would need permission to do so from the rights holders. This explosion of interest in ensuring that real-world laws are effectively translated into the virtual world will continue to challenge lawyers and lawmakers for years to come.

Who is building the metaverse?

Perhaps one of the biggest business use cases of the metaverse today is found in the gaming industry.

Take Roblox as just one example. The gaming company, which went public in March 2021, set out, in part, in its prospectus its vision for the company and the adoption of the metaverse. The goal for Roblox – as computing power, high-bandwidth internet connections, and human interface technologies improve – is to create a pervasive human co-experience platform that allows users to connect, learn, play, and work together (and even to build an economy based on its own currency, Robux). This is arguably the next iteration of Linden Lab (the creators of Second Life), which also created its own currency and which at one time had a gross domestic product bigger than that of some small countries. It is no surprise, then, that many other big names in the gaming industry are also investing heavily in their metaverse presence.

User experience in this context is just one component. As alluded to above, the word “metaverse” is derived from the prefix “meta” (meaning beyond) and the stem “verse” (meaning the universe). For the proposition of the metaverse to reach its true potential, critics agree that a number of key attributes must exist, including being persistent; able to provide live, synchronous experiences; interoperable; and value-creating. Although it is a point of debate, this means that the metaverse is unlikely to have a single entity building or operating it. Instead, many stakeholders (individuals, commercial enterprises, governments, etc.) will contribute to its existence – much like the real world.

This makes sense. The metaverse, as with the present-day internet, demands and creates opportunities for new technologies, products, service providers, content creators, standards and protocols, rules and regulations, and more, which in turn requires a community of stakeholders to build.

There is no general consensus on how the metaverse will definitely work in the future, nor who will build it or who will “own” it (if anyone). But what can generally be agreed upon is that it will exist and is no longer just a science-fiction concept. Watch this space, but don’t hold your breath for a big bang. As we know from tracking developments over the last year, the metaverse will develop iteratively over time as capabilities evolve and synergies are established. Five years ago, the metaverse was for geeks only. In five years’ time, it will be for everyone.

Authors

Olga Kacprzak
Trainee Solicitor
London
okacprazak@reedsmith.com

Arabella Murrison
Trainee Solicitor
London
amurrison@reedsmith.com

Heather Stweart
Trainee Solicitor
London
hstewart@reedsmith.com

Glossary of terms

Advertising technology (AdTech)

An umbrella term describing the tools that brands, agencies, publishers and platforms use to target, measure and analyze digital advertising efforts.

Airdrop

A marketing practice involving the unsolicited transfer of coins or tokens to numerous wallet addresses.

American Federation of Musicians (AFofM)

A labor union that represents professional instrumental musicians in the United States and Canada.

Anti-money laundering/combating the financing of terrorism (AML/CFT)

Measures to prevent criminals and terrorists from abusing the financial system.

Artificial intelligence (AI)

Machines' ability to simulate human intelligence through their programming.

Augmented reality (AR)

Enhancement of the real physical world aided by the use of technological devices to create an interactive environment.

Avatar

An icon or figure representing an individual in a virtual setting.

Binance Smart Chain

A blockchain network built for running smart, contract-based applications.

Bitcoin (BTC)

A form of digital currency that is recorded on a blockchain and is transferrable on a decentralized peer-to-peer network.

Blockchain

A distributed database or ledger comprised of "blocks," which record transactions and are securely linked using cryptography.

Collective bargaining agreements

Agreements between an employer and a union representing employees, such as SAG-AFTRA or AFofM.

Consumer protection

The protection of the public from the risks that arise when purchasing goods and services. Consumer protection legislation governs the relationships between individual consumers and businesses and covers areas such as product liability, privacy rights, fraud, misrepresentation and other unfair practices.

Creator/creator economy

A software-facilitated economy that allows creators to earn revenue from their creations, mainly on social media platforms.

Crypto-asset

A cryptographically secured digital representation of value or contractual rights that uses some type of distributed ledger technology (DLT) and can be transferred, stored or traded electronically. Cryptocurrencies, utility coins, security tokens and stablecoins are different types of crypto-assets.

Cryptocurrency

A digital or virtual currency that is stored on a blockchain and uses cryptography as a means of security. A key characteristic of cryptocurrency is that it is not governed by a central authority – examples include Bitcoin, Ethereum, Litecoin, and Bitcoin Cash.

Crypto token

A cryptocurrency that runs on top of another cryptocurrency's native blockchain. Cryptocurrencies with their own blockchain are normally referred to as "crypto coins," so this term has become a way to refer to cryptocurrencies other than Bitcoin or Ethereum.

Cyberworld

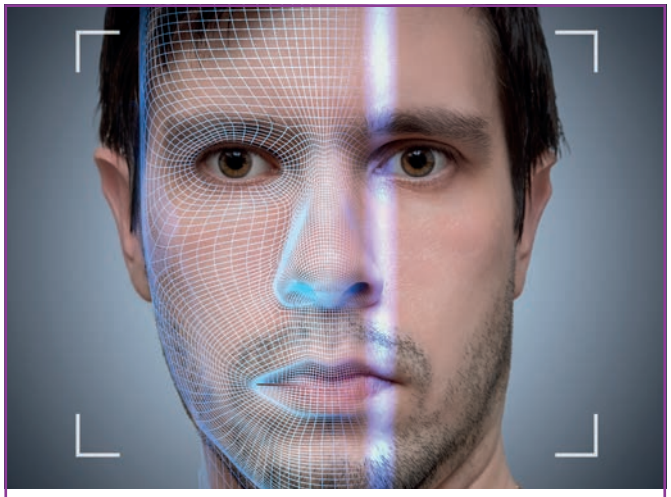
The world of inter-computer communication; a real or virtual world of information in cyberspace.

Decentralized autonomous organization (DAO)

An organization controlled by its members following rules encoded as a computer program, that is characterized as being transparent, with rules that are not permission based and without influence from central government.

Decentralized finance (DeFi)

Peer-to-peer financial services based on secure distributed ledgers similar to those used by cryptocurrencies, which work by removing intermediaries such as exchanges or banks.



Deepfakes

Content resulting from the manipulation or generation of audio-visual media by AI, often a video or sound recording that replaces someone's face or voice with that of someone else.

Digital assets

Digital representations of various virtual or real-world assets that can be owned and transferred virtually – examples include cryptocurrencies, stablecoins and NFTs.

Digital Millennium Copyright Act (DMCA)

A U.S. copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO).

Distributed ledger technology (DLT)

A digital system that enables the registration and validation of transactions on a decentralized network in multiple places simultaneously.

Ether (ETH)

The transactional token that facilitates activity on the Ethereum network and is similar in operation to cryptocurrencies, such as Bitcoin, but includes additional functionalities.

Ethereum

A decentralized platform powered by blockchain technology, most commonly known for its native token, Ether (ETH).

EU Financial Supervisory Law

A framework according to which a multilayered system of EU prudential authorities monitors systemic risks and aims to ensure consistent and coherent financial supervision in the EU.

EU taxonomy

A tool to help investors understand whether an economic activity is environmentally sustainable and meets international standards and policy commitments.

eVTOL

Electric vertical takeoff and landing aircraft.

Extended reality (XR)

An umbrella term for computer-generated environments merging physical and virtual worlds.

Fair, reasonable and non-discriminatory (FRAND) terms

A voluntary licensing commitment that standards organizations often request from the owner of an intellectual property right (usually a patent) that is, or may become, essential to practice a technical standard.

Fair use

Under U.S. copyright law, an exception that permits limited use of copyright-protected material without requiring permission from the rights holder.

Fear, uncertainty and doubt (FUD)

A particular mindset within the crypto world that is pessimistic in nature when it comes to a certain asset or market.

Financial Action Task Force (FATF)

An intergovernmental organization combating money laundering and terrorism financing.

Financial instruments

A real or virtual document that can be created, modified, purchased, traded or settled for, representing a legal agreement involving any kind of monetary value.

Financial services

Professional services involving the investment, lending and management of money and other assets.

Fractionalization

The ability to divide a blockchain token into smaller fractions, enabling it to be owned by different people.

GameFi

A game finance platform servicing blockchain games, investors and traders.

Gas

The fee, or pricing value, required to successfully conduct a transaction or execute a contract on the Ethereum platform.

General Data Protection Regulation (GDPR)

The primary piece of legislation relating to data protection and privacy in the EU and also implemented in the UK. It came into force in May 2018.

German Financial Supervisory Law

A framework according to which the operations of banks and financial service providers are supervised in Germany, and which covers aspects such as whether those institutions have adequate capital and liquidity and whether they have established appropriate risk control mechanisms.

Hold on for dear life (HODL)

A mantra among crypto enthusiasts denoting a long-term approach to cryptocurrency investing.

Initial DEX offering (IDO)

An alternative to ICO, involving launching a project through a decentralized liquidity exchange.

Initial exchange offering (IEO)

Similar to IDO, except that a project is launched on a centralized exchange.

Influencer

A person with the ability to influence potential buyers by promoting or recommending products or services on social media.

Ingestion

The process of importing data from a source to a target site for storage and analysis.

Initial coin offering (ICO)

An unregulated means to raise money for a venture to create a new coin, token, app, or service.

Intellectual property (IP)

Intangible property rights that are a result of intellectual effort. Intellectual property rights include patents, trademarks, designs and copyrights.

Interoperability

The ability for different computer software systems to exchange information, communicate with one another and "understand" the information being transferred.

Layer 1

A base blockchain network, such as Ethereum, and its underlying infrastructure, which can validate and finalize transactions without the need for another network.

Layer 2

A secondary framework or protocol that is built on top of an existing blockchain system, whose main objective is to solve the transaction speed and scaling difficulties.

Machine learning

A branch of AI and computer science that focuses on the use of data and algorithms to imitate the way that humans learn.

Markets in Crypto-assets (MiCA) Regulation

A proposed European regulatory framework, published by the European Commission in September 2020, that will apply to providers of crypto-asset services and issuers of crypto-assets.

Mining

The process by which new coins are verified and enter into circulation. "Miners" attempt to solve a puzzle, known as the PoW, with the successful miner being rewarded with an amount of cyptocurrency.

Modding

The act of making changes to software or hardware in order to create own versions.

Non-fungible token (NFT)

A unit of information recorded on a blockchain about a good or service that is not interchangeable.

Open (network)

A network that is constructed on open standard, which means it can be developed by anyone and everyone and accessed by anyone and everyone.

Patent

An intellectual property right that permits the inventor to stop third parties from using an invention.

Permissionless (network)

An open network whereby nobody is denied access or the ability to verify the network.

Personal data

Defined in the GDPR and under other international privacy legislation to cover information relating to an identified or identifiable living individual – examples include: a name, an identification number, location data, or one or more factors relating to that person's physical, physiological, genetic, mental, economic, cultural or social identity.

Play to earn (P2E)

A class of games and virtual worlds where gamers play for crypto token rewards.

Private sale

The process of selling an asset or service whereby the deal is privately negotiated directly between the seller and buyer, without recourse to an auction process.

Proof of stake (PoS)

A consensus mechanism used to confirm and verify new transactions on a blockchain. Cryptocurrency owners can pledge coins and be granted permission to authorize new blocks. It is a more energy-efficient alternative to the PoW consensus mechanism and is used by the Cardano and Ethereum 2.0 blockchains.

Proof of work (PoW)

The original consensus mechanism used to confirm and verify new transactions on a blockchain. Originating from Bitcoin, and used by Ethereum 1.0 among others, the purpose of the PoW is to prevent bad actors from infiltrating the network. It is achieved through the process of mining.

Protocol

A set of rules, or code, that enables data to be shared between computers. It is used to govern how blockchain technology functions – examples include the Hyperledger, Corda, Quorum and MultiChain protocols.

Public sale

The process of selling an asset or service whereby the asset or service is launched in the market and is made available to all customers for purchase.

Sats

Short for Satoshis, the smallest unit of Bitcoin. One Satoshi is equal to 0.00000001 Bitcoins (one hundred millionth of a Bitcoin).

Satoshi test

A method of verification in which "Satoshi," the smallest unit of Bitcoin (0.00000001 BTC), is sent to the VASP to verify the transaction and wallet ownership.

Screen Actors Guild – American Federation of Television and Radio Artists (SAG-AFTRA)

A labor union representing actors, journalists, dancers, DJs, news writers, recording artists and singers in the United States.

Security tokens

Tokens deriving their value from other assets, both physical and digital, that can be traded and are subject to security regulations like those enforced by the U.S. Securities and Exchange Commission.

Security token offering (STO)

A type of public offering of a unique digital token that represents an external asset using blockchain technology. STOs are a way of raising funding and are regulated like securities.

Shallowfakes

A method of manipulating media content utilizing simple video editing software rather than AI or algorithms.

Smart contract

A self-executing contract that exists in a blockchain network, with terms written in code.

Stablecoin

A digital currency that minimizes volatility as it is pegged to another currency, commodity or financial instrument such as the U.S. dollar or price of gold.

Staking

The process of "locking up" cryptocurrency. In exchange users may earn rewards or passive income. It is used in the "proof of stake" consensus mechanism to authenticate blockchain transactions.

Trademark

A word, phrase, slogan, design or logo that operates as an indicator of source for goods or services.

Trustless (networks)

A network whereby users can trust the information presented to them without the verification by a third party. This is because there are mechanisms in place to ensure information is verified by users within the network.

TRON

A blockchain-based operating system with smart contract functionality.

Unhosted wallet

A type of self-custody wallet that lets users keep their cryptocurrency balances independent of exchanges or third parties.

United States Patent and Trademark Office (USPTO)

An agency in the U.S. Department of Commerce that serves as the national patent office and trademark registration authority.

Utility coin

A token typically providing holders with the ability to access, via an encrypted key, a particular blockchain or network for purposes of accessing certain benefits or functionality on that blockchain or platform. Utility tokens are typically not intended for use as a currency or means of payment.

Vertiport

A takeoff and landing facility for eVTOL aircraft (similar to an airport but on a much smaller scale).

Virtual asset service provider (VASP)

A crypto exchange or platform used to transfer cryptocurrency in the market.

Virtual reality (VR)

The use of computer modeling and simulation to enable interaction with an artificial, three-dimensional (3-D) visual or other sensory environment.

Wallet

A secure location, stored on a blockchain, where a user keeps their public or private keys and passwords. The two main types are: hot wallets, which are connected to the internet, and cold wallets, which are kept offline.

Web3

A decentralized internet built on distributed technologies like blockchain and decentralized autonomous organizations (DAO) rather than centralized on servers owned by individuals or corporations. Why is it called web3? Because it's thought that it will be the third major evolution of the internet, after the World Wide Web (web1) and the user-generated web (web2, or social media).

White paper

A document released by developers that explains the technology and purpose of the project they are working on. The document tells prospective investors how the cryptocurrency was conceived and highlights its purpose.

Whale

A term used to refer to the owner (whether an individual or an entity) of a large amount of cryptocurrency who, because of this capital, is able to influence markets up or down by buying or selling.

Wrapped Ether (WETH)

The wrapped version of Ether. Wrapped tokens like WETH are tokenized versions of cryptocurrencies that are pegged to the value of the original coin and can be unwrapped at any point.

Zero knowledge proof

A cryptographic method used to protect information, in which the information revealed during a transaction is limited to that which is necessary to prove that a statement is true.

Entertainment and media in the metaverse

Advertising

Virtual worlds – each with their own culture, where consumers can adopt a different persona with behaviors and purchasing patterns that do not align with their real-world habits – provide a challenge and an opportunity to brands looking to engage in the space. The metaverse is providing an additional touchstone for developing relationships with consumers through advertising within the metaverse (think virtual billboards) from sponsorship opportunities for a virtual "bar" during a Super Bowl or virtual fashion weeks, to integrations within and creation of games (for example, Gucci x Roblox "Gucci Garden" digital multimedia experience). Done well, these direct-to-avatar (D2A) marketing opportunities can lead to digital and real-world purchases and brand loyalty.

Over the last year, brands have continued to take steps into the metaverse and integrate NFTs into their marketing strategies.

Brand- or celeb-themed artwork, memorabilia, or other assets. Brands have been integrating NFTs into various celebrity collaborations and promotions, including selling unique brand-themed assets.

Brands are buying and acquiring companies that are already in the metaverse space. For example, In December 2021, Nike acquired the NFT studio RTKFT, which produces NFT collectibles including digital sneakers. Coca-Cola teamed up with 3D creators at Tafi to auction off NFT loot boxes, which contained dynamic and rare Coke-branded NFTs, a friendship card, a vintage Coke cooler, and more hidden NFT surprises. The sales for this auction exceeded $1 million, with the goal of blending young audiences, brand nostalgia, and cutting-edge technology.

Celebrities like LeBron James, Paris Hilton, and Snoop Dogg all created celebrity-themed NFT artwork. Snoop Dogg released his NFT collection "A Journey with the Dogg," which showcased his memories over the years. The NFT drop lasted only 48 hours, with the NFTs selling for hundreds of thousands of dollars. Similarly, Paris Hilton has created over 100 NFT pieces in her collection and has hosted a metaverse party on Roblox. LeBron James has started trademarking a number of names for downloadable NFTs to create footwear and athleticwear meta merch. Per the trademark filings, LeBron will be hosting events in the metaverse, connecting users to all things LeBron James, including virtual basketball gyms and recreational facilities.

Brands are also combining the popularity of the metaverse and NFTs to showcase their fashion and history. Louis Vuitton released new NFTs in its stand-alone mobile app game Louis: The Game, where users can dress up the brand-inspired avatar and learn about the brand's 200-year history.

Charitable giving. Brands are also entering the metaverse and using NFTs to support good charitable causes. Adidas and Prada collaborated with Zach Lieberman, a digital artist, to create NFTs that feature community-sourced artwork submitted by consumers. The final NFT will be sold at an auction with the majority of the proceeds going to Slow Factory, a non-profit organization that seeks to address climate concerns and social inequities. Kith and Invisible Friends partnered to create distinctive Invisible Friends NFT characters dressed in custom Kith clothing, with the proceeds going to Kings Against Violence Initiative, a Brooklyn nonprofit whose mission is to tackle violence against young people in NYC.

Brand collaborations. Brands are collaborating together to blend each of their audiences in the metaverse. Roblox and Gucci partnered to create Gucci Garden, a digital immersive multimedia experience on Roblox. The fashion installation experience lasted two weeks on the platform. Similarly, in late 2021, Balenciaga entered the metaverse by collaborating with Epic Games, allowing Fortnite players to wear limited-edition Balenciaga skins and outfits for avatars. The items were available to buy via an in-game Fortnite currency.

Promotions. There are numerous possibilities for NFTs and promotional games. Star Atlas and The Sandbox worked together to create a metaverse contest, which could allow users to win spaceship NFTs. Further, a brand could embed an NFT in every product it sells with some of them being a surprise and delight NFT, such as entry into a virtual concert or fashion show. Brands are also exploring awarding NFTs as prizes in sweepstakes or other prize promotions. Professional sports teams are looking at developing NFTs for their season ticket holders.

Virtual experiences. Virtual experiences have become a mainstay of the metaverse. The first ever Metaverse Fashion Week occurred in March 2022, which featured events from Brands like Tommy Hilfiger, Dolce & Gabbana, and DKNY. Over 100,000 people attended the virtual event, which allowed consumers to buy digital fashion and receive a physical duplicate of the items purchased. These virtual experiences work to mimic real world events, like the Miller Lite Bar that aired a Super Bowl ad in the metaverse. Miller Lite fans could watch the Super Bowl ads while enjoying a virtual beer. Attendees could also earn limited-edition cosmetic items, with Miller Lite branding at the "bar," all of which sold out in minutes. Even stores like Lowe's are working on implementing tools in the metaverse to allow their consumers to visualize their projects virtually, which are based on real products Lowe's sells.

All of these digital world opportunities come with real-world legal hurdles (discussed in detail below), ranging from rights of publicity (see the *Content exploitation* section), to intellectual property (see the *Intellectual property* section), to SAG-AFTRA and other union obligations (see the *Music* and *Content exploitation* sections).

Authors

Stacy Marcus
Partner
New York
smarcus@reedsmith.com

Jason Gordon
Partner
Chicago
jgordon@reedsmith.com

Keri Bruce
Partner
New York
kbruce@reedsmith.com

Emily R. Faro
Associate
New York
efaro@reedsmith.com

Sara Mohammed
Associate
New York
smohammed@reedsmith.com

Games: An NFT-powered revolution?

A lot of what the metaverse looks like comes from the world of video games. Second Life, the iconic game from Linden Lab, is arguably one of the oldest metaverses on the internet. In future, you may enter games through a headset and feel them through a haptic suit, but at their core, the experience of entering a metaverse is likely to bear many resemblances to how players today immerse themselves in Second Life, Roblox, Fortnite, or Minecraft.

On the other hand, web3 adds a far more disruptive element to the picture: the inclusion of decentralized technology, blockchain, and non-fungible tokens (NFTs). The world of crypto games is growing fast and is slowly spanning another sector altogether.

So, what will change?

Web3 games are powered by blockchain technology and decentralized governance regulated by smart contracts, allowing players to collect game-specific assets in the form of NFTs. Play-to-earn allows players to earn rewards in the form of NFTs, which can be exchanged for cryptocurrencies that can be converted into fiat currency. One of the first "play-to-earn" games in the cryptocurrency market to really gain traction was Axie Infinity. Axies are token-based creatures that players can collect, breed, nurture, battle, and trade.

Axie Infinity is a prominent example of how the business model behind video games is being re-invented by web3. Web2 games used to measure their success based on player engagement since the more time someone spends in the game, the more likely they are to purchase in-game assets. Web3 play-to-earn games add a financial incentive to that time. NFT-based games promise to make the labor of fun into compensated labor, and some even claim that they are training the workers of the future - as humanity moves closer to living and working in the metaverse. In a play-to-earn model, the more players play, the more money they earn. In Axie Infinity, the basic cycle of gameplay works like this: completing levels creates stronger Axies to win matches, which provides players with tokens that allow Axies to "breed" and thus create new Axies to be sold or used for play.

The NFT opportunity

Video game makers are all looking at NFTs, and the topic leaves no one indifferent. Large companies like Ubisoft have already taken the first step and are creating their own proprietary line of NFTs to be used in their game properties, while others, like Mojang, the studio behind Minecraft recently decided to ban them from their game, arguing that "NFTs can create models of scarcity and exclusion that conflict with the Guidelines and the spirit of Minecraft."

For game makers, incorporating NFTs into their business models has potential. NFTs can be sold to players in the same way other downloadable packs can: as a product sold from a store, where the initial sale includes a profit for the developer. But these tokens can be coded. And it has become a feature of NFT smart contracts to allow each resale to automatically trigger a payment to the originator of the token – in this case, the game developer. The model allows game makers to monetize items again and again, using the prospect of future player-to-player sales to generate an ongoing revenue stream.

Play as labor

The lines between play and labor in video games have long been blurred. For example, Eve Online, a massively popular multiplayer online game, is a 19-year-old game that is reliant on player labor to generate new items in the game and to keep the in-game economy flowing. Players of Eve Online lead and work on various spaceships, which can be optimized for either mining in-game resources or building specialized combat vessels. Once enough materials are mined, they can be sold in a marketplace for real-world currency, and the raw materials can be crafted into new spaceships.

In many online games, players have to "do a job" to advance through the game world. But the "grind" of doing repetitive or time-consuming in-game tasks unlocks better characters, new levels, or skins rather than real-world money. "Playbor" is a term that was coined by researchers to describe the behavior of engaging in ordinary play that also generates income, whether virtual or real. Whether players earning money from playing a game count as employees, contractors, or neither has created an unregulated space that will undoubtedly brush up against employment law in a near future.

Protecting and educating players

The incorporation of NFTs into games restricts access to those players feeling savvy and confident using complex, not-easy-to-understand, and volatile financial instruments. Players of web3 games are therefore exposed to financial risks. The safeguards, which may well be needed to protect the most unsophisticated players from being manipulated or hacked (for example, by approving trades they don't understand), may come from finance regulation, but clearly call for consumer law regulation, too. The Axie hack earlier this year is indicative of the risks built into the evolving nature of video game marketplaces, and it demonstrates the need for regulators to implement better monitoring and consumer protection schemes.

Perhaps in response to these risks, some video game publishers are putting their own restrictions on the ways in which games can incorporate cryptocurrencies. Steam, the largest digital storefront for PC games, made a stand by banning all blockchain games from its platform and updating its policy documents to reflect the change, thus placing a huge barrier to wider adoption of the technology in games. The co-founder of Valve, the company behind Steam, cited the high volume of fraud and scams being perpetrated through crypto-assets like NFTs as the motivation for the ban. In contrast, Epic, the publisher of Fortnite, has said it is open to cryptocurrencies and NFTs in its game stores, but only if they strictly adhere to reporting and tax laws.

Looking into the future

Multiple countries are starting to tax cryptocurrency transactions and have imposed due diligence and know-your-customer rules on crypto exchanges. These regulations are meant to make crypto-assets trade, including NFTs, “safer,” but as ever, implementing national rules to worldwide endeavors continues to cause major headaches to regulators and it may be a few years before we see the effect of these policies.

It remains to be seen whether play-to-earn really does become the future of gaming, and whether NFTs will be at the centre of it. Clearly, some players are attracted to the idea of unlocking “better” property rights for their in-game assets, but for others, including parents of young players, safety and fun are values that may not be compromised. As of today, web3 games seem far more likely to develop into their own new sub-sector than disrupt a flourishing and mainstream games industry.

Games and metaverse issues

The infrastructure prerequisite. For the metaverse to be an alternative to the real world, it's going to have to resemble it with almost complete verisimilitude. Luckily, there is no need for governments to pour trillions of dollars into this sort of infrastructure. The processor and graphics technologies have been incentivized by a red-hot video games market for years, and today we inch closer and closer to absolute realism. Intellectual property and licensing issues will increasingly dominate the conversation as publishers and console manufacturers design and build with those technologies.

Because video games can be seen as prototypes for the metaverse, it is impossible to escape the inherent limitations of that model when applied to a vision of interoperability. In some ways, the NFT and related tokenization issues are relatively more solvable than those that relate to the underlying infrastructure of the metaverse. Do we have any more reason to believe that the metaverse will resemble one planet on which all human life can love, hate, fight, reconcile, exploit, and heal than we believe one gamer account (e.g., its crypto wallet) can be used across all games and all platforms? It is the promise. The intellectual property and attendant license are far more likely to result in multiple metaverses,

"Whether players earning money from playing a game count as employees, contractors, or neither has created an unregulated space that will undoubtedly brush up against employment law in a near future."

divided at least by platform configurations if not also by content, genres, and publishing rights. The profit incentive that has ignited the development of the technology will be the very reason the technology will form walls around competing worlds. In this sense, the video game model for the metaverse foretells the limits that are baked into the infrastructure that will form the metaverse.

There may be those who envision a metaverse that transcends the boundaries of jurisdiction and platform, but they will run headlong into the reality of intellectual property, antitrust, privacy regulation, and the capitalistic spirit that has powered the video game industry for decades. And, speaking of power, the infrastructure for the metaverse is again going to bring with it questions about the energy usage required to run the processors and graphics chips. Video games and the infrastructure providers who pave the way for the next generation of games and, perhaps, some version of the metaverse again provide a useful guide. Energy usage and issues surrounding sustainability and conservation will become distinguishing factors for companies competing for adoption in games and platforms. With public opinion on a global basis appearing to bend toward a joint goal of sustaining our planet, those seeking to drive the video game experience toward complete immersion will likely need to consider how to be ecologically responsible (both in terms of energy usage and use of sustainable construction materials) rather than just create larger and more voracious appetites for the Earth's resources.

Human nature and the limits of moderation. Another lesson from the online world of video games is that unchecked, they can devolve into dangerous places. The recent adoption of the Digital Services Act in Europe has been hailed as the biggest change to internet laws in a century – placing an onus on all streamers and user-generated-games companies to protect their users, and in particular children, from harassing, bullying and harmful content. This EU initiative will complement other initiatives taken by other jurisdictions who are likely to be measured against the new EU standard.

In the UK, the Information Commissioner's Office (ICO) Age Appropriate Design Code, which became effective in September 2021, focuses on the processing of personal data of children (up to the age of 18) and recommends certain default settings for services that are likely to appeal to children, including taking into account the best interests of children when designing any data processing in services; providing a child-appropriate service to all users by default, with the option of an age verification mechanism to enable adults to opt out of these safeguards; identifying the ages of children by using robust age-verification measures; providing all relevant privacy information, clearing terms, and community standards by using age-appropriate design codes and appropriate content presentations that can be easily read and understood by children; and prohibiting the use of data that is detrimental to children's physical or mental health and well-being, or goes against industry codes and government regulatory provisions.

In Germany, the Federal Protection of Young Persons Act (Jugendschutzgesetz - JuSchG), effective from May 2021, is aimed at the protection of children and young persons against harm resulting from media use and to ensure that media is only distributed or made available in accordance with the applicable age rating. This includes media and other publications with, among other things, immoral and violent content; presentation in detail of acts of violence, murder, and massacre for their own purpose; or a recommendation of the "law of the jungle" as the only proven tool by which to obtain supposed justice.

In the United States, the Child Protection and Sexual Predator Punishment Act (CPPA) and amendments via the Securing Adolescents From Exploitation-Online Act (SAFE) create several duties for online service providers, including a duty to report evidence of apparent child exploitative activities of which the provider becomes aware. The penalty for knowingly and willfully failing to report can result in an initial fine of $150,000 with subsequent violations carrying a fine of $300,000.

The law provides a limitation of both civil and criminal liability for providers performing reporting or preservation responsibilities under the statute. Beyond this specific law that focuses on sexual predators who might be engaged in criminal acts in a context such as a virtual world, the U.S. Congress appears to have an appetite to revisit section 230 of the Communications Decency Act. Possible changes to section 230 could include incentives for online platforms to address illicit content and create exemptions for immunity in the areas of child abuse, terrorism, and cyber stalking.

The world of video games is increasingly being subjected to governmental oversight to address online harms – at least in the context of children and teens. We have also seen signs in some countries that suggest a willingness to push more liability onto platforms if their programmatic moderation mechanisms fail to moderate content that is deemed to be offensive or unlawful. The fact that dangers can present themselves in various interactive media contexts, including interactive video games, and that regulators in many countries have taken affirmative steps to address them suggests that the metaverse would be subject to similar considerations.

Yet, in the metaverse, it is unclear whether governments could reasonably seek to regulate or promote the sort of moderation that they currently do in the context of video games. If the concept of "platform" becomes fully decentralized, what liability could attach to a foreign developer who does not impose anti-online harm moderation? Would national regulators need to engage in the virtual world, almost like Agent Smith in "The Matrix?" The limitations of moderation in a decentralized metaverse conception pose interesting questions about the governance of the world we are building for our children.

Authors

Sohie Goossens
Partner
London
sgoossens@reedsmith.com

Nick Breen
Partner
London
nbreen@reedsmith.com

John Feldman
Partner
Washington, D.C.
jfeldman@reedsmith.com

Music

As one of the first of the content industries to be heavily disrupted and changed beyond recognition in the early days of the internet, in many respects, the music industry has, since the turn of the century, been one of the first to adopt change and new business models online.

When the possibility of performing and delivering live music performances to large crowds disappeared almost overnight with the advent of the COVID-19 pandemic, the music industry and, particularly, performing artists were forced to innovate and find new ways to reach their fans. Naturally, they started performing online. It is worth noting at the outset of this discussion that online livestreaming is not a new thing – the Rolling Stones were doing it in 1995, and many companies were delivering livestreams of musicians, including internet pioneers such as AOL and Yahoo!, long before musicians started using platforms provided by modern players like Twitch and Facebook.

Several defining characteristics distinguish this new form of music consumption in the metaverse from traditional "vanilla" livestreaming or even subscription streaming:

- A walled-garden platform environment
- The ability to build, style, and control, or just perform in, a virtual venue
- The possibility of using an avatar or other visual representation of the artist, sometimes comingled with a true video representation of the artist
- New production capabilities, including manipulating the virtual environment and combining digital visual production with the artist's own musical production
- The ability to interact with the audience in real time
- In some instances, the combination of more than one artist performing from a different location or virtual venue

There have been many fantastic examples of this innovative musical art form in recent years, but perhaps the most striking and commercially successful was the Travis Scott performance in the Fortnite video game. The traction and audience for this event were phenomenal, with Scott himself commenting: "It was an opportunity to go to the max, to create a world that permits won't let you do, fire marshals won't let you do, building codes won't let you do." Little did he know that these comments would gain prescience after a tragedy at one of his concerts involving people in real life. Where Scott started, others followed; Future, Zara Larsson, Ariana Grande, and other superstars have pursued performances in virtual environments.

Aside from virtual events and NFTs (covered elsewhere in this guide), another metaverse phenomenon affecting the music sector has been the emergence of virtual "artists." While the idea of engaging with a virtual artist, created by artificial intelligence and not having a human personality, may be anathema to many true music fans, there is no denying that such artists are gaining huge traction among digital natives. We've already discussed FN Meka, described as a "robot rapper who is known for his extravagant style and Hypebeast aesthetics. He has the appearance of a cyborg with green hair and eyes, lots of tattoos, and a hand made of gold." While this may all seem to be a bit of harmless, somewhat futuristic fun, it has a foundation of serious commercial potential, as FN Meka's fanbase shows. As a means of comparison, at the time of this guide, Chance the Rapper – often spotlighted as one of the new breed of superstar rappers – has only two million TikTok followers compared to FN Meka's 10 million.

Is the metaverse an opportunity or a threat to music?

As the prominent examples above demonstrate, the metaverse can be an opportunity and a threat to the music industry. Certainly, as the production and experiential capabilities of technology continue to push boundaries and create new consumer experiences, artists who rely on old-style production techniques and traditional channels to reach their audiences risk getting left behind. Some of the more one-dimensional approaches to the music industry – such as purely owning rights and monetizing through subscription streaming channels – will quickly become commoditized and mechanized to the extent that they don't yield the profit margin to make them worthwhile.

Meanwhile, the commercial promise available to those who are prepared to push the boundaries and use all of the available technology to engage and create is galactic. Even the biggest arena tours cannot accommodate anything close to the instant, one-time global audiences that can be attracted to an online metaverse performance. The COVID-19 pandemic, which forced the world to migrate online for entertainment, has shown the music industry that ticketed, cleverly produced, and engaging livestreaming will be here for the long term. It is likely that the most significant concerts and festivals that happen in the real world will, in the future, have a more dedicated, slick, and transactional online component. For that reason alone, the metaverse is here to stay in music.

More interestingly, we can already see that the combination of virtual value tokens and music is a match made in heaven. Companies are furiously trying to work out how to enable fans to invest directly in their artists and engage with them in a way that enables value exchange and support. Royalty streams could be fractionalized, with the blockchain underlying such royalty streams acting as a permanent record of who gets paid, and how much.

What are the legal issues for music in the metaverse?

As always in music, the primary consideration when music is created, performed, streamed, and exploited online is rights clearances. Mostly, the traditional legal and licensing rules applicable to online exploitation apply equally in the metaverse. However, the proliferation of music, performance, and exploitation within new, closed, or even open online environments adds yet another potential layer of complexity to an already complex chain of rights in the music licensing process.

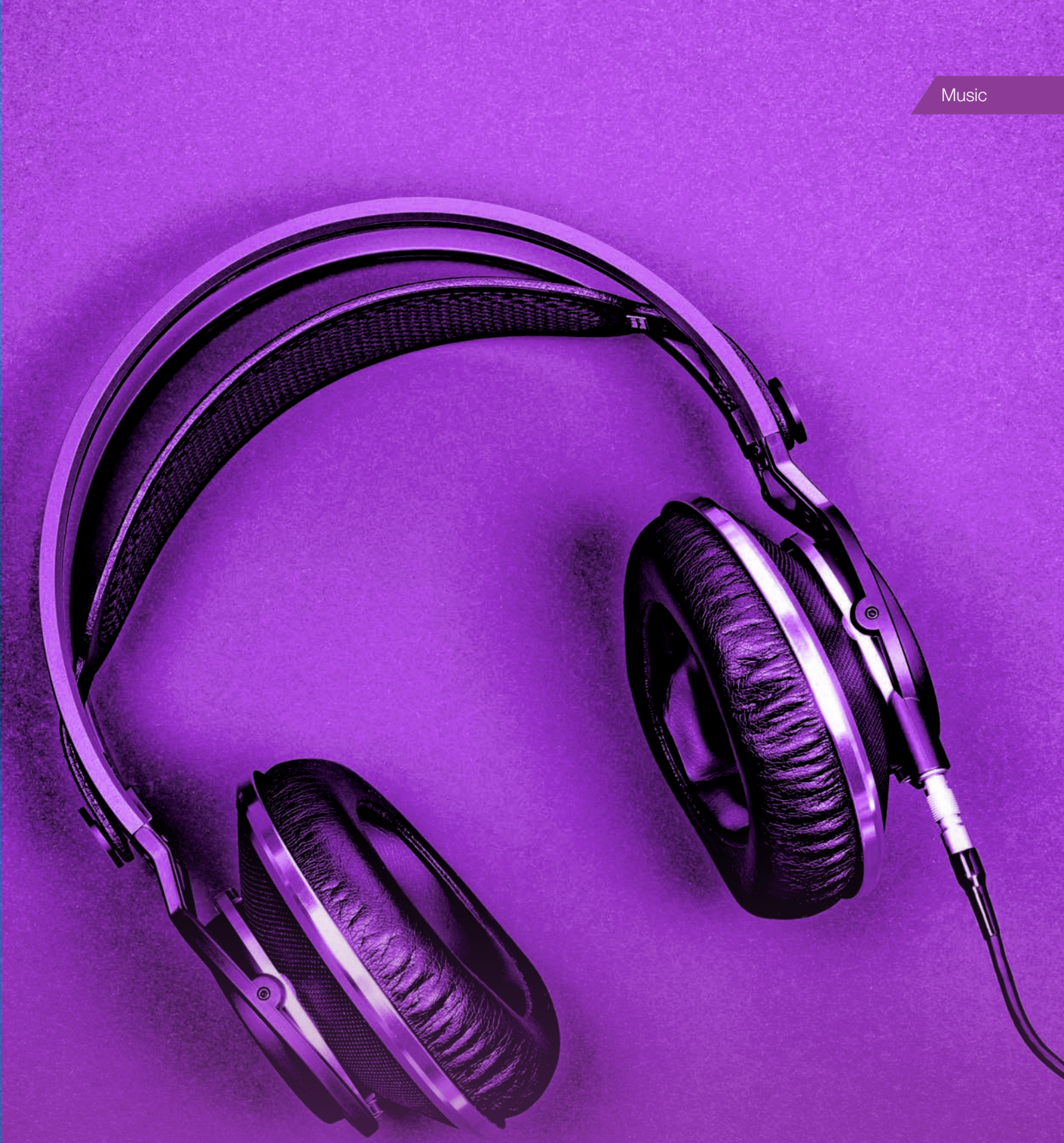
To take an example, a digital music service provider (for instance, Spotify) could promote and host a live-streamed concert on a global games console platform (let's say, Sony PlayStation) during the interval of an eSports tournament being held and promoted by a leading games publisher (perhaps, Electronic Arts) working alongside a famous brand (maybe, Nike). To attend the concert, a consumer would need to be a user of the gaming platform and have purchased ticketed access to the eSports tournament. However, the live-streamed concert would only be available to a limited number of superfans who had entered a prize draw by buying an original NFT token issued by the headline performing artist (for example, Drake). Prizes might include, at the top level, attendance at the live virtual event and an authentic piece of digital merchandise, while runners-up might still get to see the concert on an on-demand basis at a later date, missing the live show.

The network of contractual obligations to navigate and the rights-clearance issues to think about that are illustrated by the example above are not wildly different from the issues that lawyers may be dealing with in the real world. The half-time performance at the NFL Super Bowl is well known in the music industry for being a highly prestigious, but complex, production and clearance exercise. However, in many respects, the level of complexity associated with clearing music and artist imagery for the metaverse can be significantly more complicated.

Walled gardens. If we accept that the metaverse, particularly looking forward, is made up of one or more dynamic environments in which we can interact and enjoy experiences, the obvious question is, how can each environment be regulated legally? In the early days of the virtual world of Second Life, disputes were common. In the 2000s, the discussion among lawyers concerned whether "virtual laws" could exist and whether avatars could find new freedoms to exploit their creations (or adapt and copy other people's creations). The law has since moved on considerably; it is now more widely accepted that online environments are subject to offline laws. Any platform or environment of scale will be careful to prescribe the contractual terms on which users are permitted to use the platform or environment. Therefore, the use of music within a metaverse region will be subject to the terms of service applicable to that environment. Then, anyone seeking to use someone else's music in the metaverse will need to be sure that the terms under which they obtain a license align with the terms of the walled garden in which the music is used. While this sounds easy in principle, a truly global virtual environment is regulated differently, according to the legal jurisdiction. Censorship and content standards affecting a live performance of a leading rap artist will be vastly different in the United States from, say, Indonesia, Dubai, or Hong Kong. Artists often have political views and make statements onstage (who remembers Rage Against the Machine's protest against Guantanamo or Sinead O'Connor ripping up photographs of the pope?). These types of incidents are more containable in real life, but they are the stuff of nightmares for the legal compliance teams at big platforms who often seek to maintain good relations with local governments around the world.

Who clears the rights – I'm a user. It could be argued that consumers are accustomed to the platforms themselves covering music licensing, at least from a performance or communication to the public standpoint. Online services that have been reported to benefit from blanket licenses with music rights owners and collection societies include Twitch, Facebook (reference here and here), YouTube, TikTok, and PlayStation. Notwithstanding that such platforms are clear in their terms of service that music licensing is the responsibility of the uploader, at least consumers can feel more comfortable about using music in the environment in which they are operating.

However, things become more nuanced when music can be created, shared, and enjoyed in a real-time gaming metaverse or social environment. The tools by which any user can now instantly manipulate, edit, and deliver an entirely new musical creation by simply creating a meme are widely available and can be used to devastating viral effect. Whoever came up with the dance challenge to Jawsh 685's "Laxed (Siren Beat)" could not have anticipated that a song created by an unknown New Zealand artist in four hours as a tribute to his Samoan heritage would soon become one of the world's biggest hits, subject to a dispute over a sample featuring Jason Derulo, and become a number one hit song around the world. At the time of writing, TikTok is unarguably the most important platform for breaking and promoting new music, but now more than ever, it is users who are dictating whether and how a song catches fire. For lawyers advising artists, labels, publishers, and even the platforms themselves, the viral capacity of user-created mashups and multiple synchronizations creates never-ending potential for innovative licensing solutions, disputes, and lucrative transactions.



“As always in music, the primary consideration when music is created, performed, streamed, and exploited online is rights clearances.”

Who clears the rights – I'm an artist. Reflecting on legal issues affecting music users in the metaverse is to say nothing, of course, of the tripwire territory created by the implementation of article 17 of the Copyright (Digital Single Market) Directive when it comes to music in the metaverse. By way of reminder, article 17 was the mechanism by which the music industry sought to make it compulsory for video platforms to obtain sitewide licenses as opposed to relying on safe harbor exceptions. While this goal may now have been achieved – and, in fact, arguably the majority of Western video platforms were already licensed or in the process of obtaining licenses when the new laws were finally ratified – the law of unintended consequences may now be taking effect when considering the scope of what those platform licenses should cover. To recap (and to grossly oversimplify), while the platform will be responsible for making efforts to obtain licenses for content uploaded by users, it will not be held responsible for licensing copyrights in content that is brought to a platform by commercial operators. In the context of music, this immediately raises the question of when an artist is a "professional user."

Who clears the rights – I'm a promoter. Artists as diverse as Ava Max, BTS, Marshmello, and Kaskade have performed through graphic representations in online gaming environments, while cutting-edge virtual reality services like MelodyVR (now rebranded as the next-generation Napster) and Facebook's Oculus permit users to view real-life concerts in a virtual reality format in real time. There is no one-size-fits-all approach to clearing rights for these types of events; much will depend on:

- The artist performing
- The basis on which the artist's recording and ancillary rights are managed
- The songs or compositions that will feature, including whether those recordings were produced under the SAG-AFTRA Sound Code
- Production components that are included (for example, choreography – formerly the preserve of only the most diligent of production rights clearance professionals – can now be a total minefield in the metaverse environment)
- The virtual engine powering or underpinning the production
- The creative input from digital artists and other virtual contributors

In more straightforward production environments, those responsible for delivering clearances and "legals" for an online concert can follow tried and trusted video production methodologies, supported inevitably by a music clearance house that can gather together the myriad reproduction licenses needed if the concert will be recorded and exploited. At the other end of the spectrum, however, lawyers are having to develop skill sets that combine (a) the copyright and intellectual property licensing disciplines associated with video game production and game studio development; (b) technology and software licensing expertise, especially where multiple platforms or SaaS (software as a service) products are used to power a virtual, avatar-driven performance; (c) rights acquisition and capture for proprietary elements; and (d) old-school live music performance clearances.

Fence hopping. Once the preserve of fantasists, but perhaps now more likely than ever before, it could soon be the case that a user's avatar can move between environments. Do you want your World of Warcraft character to play in Fortnite? Could Super Mario fight with Sonic the Hedgehog? That may happen. In such a scenario, metaverse environments will need to find new ways of clearing music. Similarly, if a user has a Spotify account, they may like to listen to their music playlists while playing multiple games, perhaps even in a seamless manner. Traditional music distributors – and remember that Spotify is more than 13 years old – may need to play catch-up to ensure that their services don't get swallowed up by the metaverse. Ideas that would have sounded like pure fantasy from a legal perspective 10 years ago are now fast becoming a reality that could burden lawyers for years to come (for example, creating a coffee shop in a virtual world where users can get together and listen to and share their music).

Creating new music in the metaverse. Of course, if people are going to exist, project their images, and spend their time in the metaverse, the next logical step for them is to move out of the real-life recording studio and into the virtual creative environment. Already, there are extensive examples of this taking place. VR headsets and controllers that allow users to interact with graphical interfaces that represent musical instruments are widely available. Literally, the air guitar becomes a real guitar - Rock Band VR anyone? Forming your own band online, transforming yourself from a balding, middle-aged guy with a "dad bod" into a lavishly coiffured, tanned, lithe rock god, and living out your fantasies of playing guitar in front of huge crowds is now completely possible. On a more prosaic level, metaverse environments such as Minecraft, Roblox, and Fortnite contain song codes, instruments, recording tools, and music manipulation controls that enable users to be musically creative. While the majority of this activity will result in original copyright that will be of almost zero monetary value, there are infinite possibilities for users to unwittingly infringe or encroach on well-known commercial songs or properties. Do you want to perform a Whitesnake track with your virtual buddies, only to a drum and bass beat and combined with lyrics from Dizzee Rascal, while playing your virtual DJ decks and sharing your live set with your new metaverse friends in Bangalore? No problem.

Of course, when the combination of creative technology, people, and connectivity moves up a gear, so do the legal issues. Music is already one of the most byzantine, challenging, and disparate areas of entertainment law.

The prevalence and expansion of music in the metaverse certainly presents new challenges, but it also creates massive opportunities for legal professionals to innovate and help their clients – not only to navigate through the existing frameworks but also to create new models and ways of exploiting copyrights that help drive incremental revenues and value to the industry, artists, creators, and the platforms that invest in the metaverse itself.

What about music NFTs?

While we have covered NFTs in general in other parts of this *Guide to the Metaverse*, it would be remiss of us not to explore how the music industry is taking advantage of this technology.

Music NFTs have the potential to allow artists to build scalable, customizable offerings to engage and reward their fans. Artists will have access to a decentralized database of their core fan base that they can choose to reward over time without being at the mercy of a centralized platform to do so. We will begin to see how artists take advantage of this as music NFTs reach mass adoption. For instance, perhaps an artist will airdrop a free NFT to fans that have collected all of the artist's NFT music releases that will grant holders access to an unreleased track. Maybe fans that have gone to see the artist numerous times and have more than 10 proof-of-attendance NFTs in their wallet will be invited to an intimate private gig.

While there are limitless applications for NFTs to transform the music industry, from ticketing (such as GUTS Tickets), unique collectibles (such as Serenade), distribution (such as Audius), and beyond, two forms of music NFTs have been subject to much debate and discussion:

Tokenized ownership. A growing number of web3 businesses are exploring tokenizing underlying copyrights and/or royalty income streams (such as Royal, Opulous, etc.). Conceptually, fans acquiring proprietary ownership of rights to their favorite artist's music is certainly compelling and arguably allows early fans to ride the wave of an artist's success.

As you may suspect, there are numerous legal and practical issues that arise from these offerings, the most obvious of which is the extent to which such offerings are regulated as investment products or securities. It is fair to say that the answer to this question is not straightforward, and the outcome will be highly fact dependent. Businesses will need to keep abreast of international regulatory changes, as regulators start to establish what is and is not within their remit. We have considered this in further detail elsewhere in this guide.

Music NFT editions. Web3-savvy artists have taken full advantage of selling their music as NFTs directly to fans through music NFT platforms (such as Sound.xyz). With little to no take-rate applied by these platforms, artists are making significant sums from selling these limited-edition digital versions of their music.

With money to be made, we are beginning to see the various music stakeholders take their positions. Eager not to be left behind by the latest technical innovation, labels and publishers alike are already updating their artist agreements to accommodate NFTs.

Who has the right to issue and sell a music NFT? What rights need to be cleared in a music NFT? Who needs to clear those rights? And, most importantly, who is entitled to proceeds from sales and in what proportions? The answer to most of these questions comes down to a simple analysis of basic copyright principles – assessing what copyright-restricted acts are being undertaken (if any) and by whom. Nevertheless, a key battleground between stakeholders will concern who gets paid what. We anticipate renewed arguments about what amounts to a "sale" or "license," whether NFTs are a new format, and whether there is a "sync," etc. Although on the face of it, everything is up for grabs, our view is that traditional rules and common sense will prevail.

What about investing in music using web3 technologies?

Notwithstanding an increase in the cost of capital in 2022 amid soaring inflation and rising interest rates, the corporate appetite for acquiring music copyrights at scale shows no real sign of abating. Partly, this appetite has been due to excess liquidity in the finance market and the strong revenue growth exhibited by music catalogs, in turn, due to a combination of better, more accurate distribution technologies and the growth of subscription streaming services like Spotify.

Web3 threatens to further disrupt the market for music copyrights. There are several companies either exploring or offering investment models via which members of the public can "invest" in the creation of new music in return for a fractionalized share of royalty revenue received from the exploitation of that music. These models typically work by a combination of (i) users paying money for the opportunity to fund or invest in an artist's work, by paying in cryptocurrencies toward the artist's costs of creating the music; and (ii) users receiving a token in return, which is intended to represent a fractionalized share of the overall royalty stream that is to be received from the track.

Although the idea of consumers being able to "invest" in music is not new, these models raise a number of legal issues:

- The offering of investments or the conducting of activities that are targeted toward the general public as investments are, understandably, heavily regulated. In many countries, it is illegal to offer investment opportunities unless through a heavily regulated business. Any entity that seeks to offer fractionalized royalty interests is likely to be subject to regulation. Some operators in the space seek to establish themselves as offshore businesses in favorable jurisdictions in an effort to indirectly avoid regulation.
- Traditional music distribution models don't lend themselves well to disaggregated royalty collection and distribution. In order to achieve a legitimate fractionalized royalties model, rights owners may need to transfer certain rights to the operator of the business and sign letters of direction or other instruments via which the artist's and even the label's or publisher's right to receive monies is instead assigned to the entity responsible for paying out a fraction of the royalties.
- There are abundant opportunities for fraudulent behavior, whether by the artist or creator, the consumer, or even the site or service operator. There is no centralized or globally recognized mechanism for preventing fraud or dealing with financially abusive conduct.

Although blockchain technology lends itself well to enabling the completely accurate distribution of royalties, many of the legal issues associated with fractionalized or automated investment models in music are difficult to overcome and may ultimately render such activities impossible in the longer term.

Authors

Gregor Pryor
Partner
London
gpryor@reedsmith.com

Nick Breen
Partner
London
nbreen@reedsmith.com

Film and TV

The film and TV sector is famously nostalgic: Hollywood loves glorifying its own golden age, and in the past has been accused of struggling to embrace change. And yet, the technological framework surrounding the industry is advancing faster than ever before.

How, then, does the industry reconcile this apparent inflexibility with the advent of the metaverse? The short answer is: tentatively. We are still in the early stages of change creeping into the sector, but already some of the potential is clear to see.

NFTs and financing

The three letters are unavoidable when discussing the metaverse, and the legal implications of non-fungible tokens (NFTs) generally are covered in ample detail elsewhere in this guide. There is no less potential in the film and TV space than other media industries – though perhaps some of that potential remains more untapped when compared to music and video games.

Financing is the most obvious area of production where we might see swift incoming changes. A handful of independent films have already been funded with NFTs, each representing a small ownership share in the project.

Film financier, The Forest Road Company, has also recently closed a $20 million fund of pre-production investments, and will issue collectibles based on the IP of each of those productions, using NFTs. It remains to be seen how this will tally up with the big institutional financiers, particularly banks, which are notoriously conservative in their approach to media financing.

NFTs and distribution

NFTs also present a new route for distribution – in other words, releasing content itself as NFTs. Conceptually (and legally), this works in the same way as it would for a piece of digital art, although it is perhaps more difficult to fathom its acceptance by the wider public for now.

Still, Mila Kunis's production company recently produced a web series, "Stoner Cats" (yes, you read that correctly), then sold NFTs granting buyers the right to watch episodes, and made over $8 million in 35 minutes in the process (yes, you also read that correctly). So the hype is definitely there, and it is valid.

But a far more feasible, widespread application would be to use NFTs as a way to exploit existing IP in novel ways. Creators can leverage the inherent scarcity of NFTs to generate exclusive products to bolt on to traditional productions – think bonus content, digital posters, commentaries, specialist cinema tickets, and so on. And because of this potential value, we have seen a spike in the number of negotiations centered on the grant of NFT rights (and the exploitation thereof) between the rights holder of an underlying property and the acquirer of those rights looking to develop and/or exploit the property through an audiovisual production. Historically, such rights would have been customarily (or at least arguably) included in the broad grant of rights provisions included in the chain of title documentation. And because of the

potential financial windfall of exploiting NFTs, we have also seen an increased demand to revisit the old chain of title documentation for a determination of who owns what rights (studios want to confirm that they have control over their exploitation, and rights holders want to confirm that they have been reserved from the relinquished rights.) A leading example of why this has become a hot topic is the recent lawsuit between Miramax and Quentin Tarantino regarding the NFT rights to Tarantino's screenplay for "Pulp Fiction."

However, the concept is still in its infancy, and the press is eager to spot early adopters' mishaps. Seth Green was planning to develop and produce a show based on a "Bored Ape Yacht Club" NFT that he had bought, in line with the usage rights he had acquired along with the NFT. Unfortunately, those plans have been shelved for now, as Green fell victim to a phishing scam in which a hacker gained access to the NFT and sold it to a third party.

Metaverse early adoptees

It is clear that the utilization of the metaverse will continue to grow in the coming years, and as it does, studios and streaming platforms need to be prepared to compete for subscribers and for the attention of their target audiences, which is why we have seen some big players beginning to dedicate significant resources to the space and how to leverage it. In particular, ViacomCBS (now Paramount) has made a pointed move toward embracing all things metaverse, creating a "futurist-in-residence" role for executive Ted Schilowitz, and toying with the idea of using and reimagining their vast, valuable IP universes in the VR and AR spaces.

Elsewhere in the metaverse, feature-length content is starting to flirt with the new worlds we are seeing unfold. The Sundance Film Festival has been an early adopter of the metaverse, seeking to showcase films that push the limits of traditional cinema. For example, "We Met in Virtual Reality" was a documentary film shot entirely within the social platform VRChat – featuring real characters and real stories, being played out in an already-developed corner of the metaverse – and that received widespread critical acclaim during its premiere at Sundance 2022.

In the end, we think the metaverse will be embraced by the film and TV community (and not replaced by it), providing studios and production companies an opportunity to engage their audiences in an unprecedented manner (e.g., enhanced viewing experiences, interactive content, and virtual worlds built around a foundation piece of audiovisual content that fans can visit and engage with for marketing purposes).

Legal implications

The film and TV industry is, for the most part, still in the idea stage of adopting web3. The potential is there, and one need only look at the other media sectors covered in this guide to see the sheer variety of opportunities that the metaverse presents to all creative work, including the audiovisual space.

Crucially for film and TV, new methods of exploiting existing IP presents an opportunity for additional revenue sources, and that optionality will continue to be a topic of negotiation in rights deals. The potential interactivity with viewers also creates an exciting – but legally complex – prospect.

As ever, new formats will create new tensions between rightsholders and licensees. The *Content exploitation* section of this guide unpacks the myriad legal issues facing exploitation of audiovisual content in the metaverse in more detail.

Authors

Christian Simonds
Partner
New York
csimonds@reedsmith.com

Henry Birkbeck
Associate
London
hbirkbeck@reedsmith.com

Legal issues in the metaverse

Intellectual property

We already understand that the known universe of the internet has caused a great number of models that take advantage of intellectual property rights to converge – challenging owners and users of protected content in the areas of authorization, monetization, and enforcement. The metaverse and web3, conversely, will likely continue to challenge the relevance of some of our core IP mechanisms, put others – like interoperability - under the spotlight and redefine the proprietary nature of technology, virtual worlds, virtual assets and our "things" in the metaverse.

Software interoperability

The purpose of interoperability is to enable different systems to "talk" and "understand" the information they pass to one another. Although it is valuable in any field, interoperability is especially relevant for the metaverse, where no single software will be used to build it.

In legal terms, interoperability is a concept that limits the rights of computer program rights holders, which are protected by copyright. In effect, their authorization is not required where copyright-relevant acts pertaining to the code are "indispensable" to obtaining the information necessary to achieve the interoperability of an independently created computer program with other programs, provided that certain conditions are met (legitimate access to the software, necessary acts only, etc.).

Today, the concept is increasingly coming to the fore, with the creation of the Metaverse Standards Forum by several big tech names (Meta, Adobe, Microsoft, Epic Games, Ikea, Sony, Nvidia, etc.) to "foster the development of open standards for the metaverse." "The Forum will explore where the lack of interoperability is holding back metaverse deployment and how the work of Standards Developing Organizations (SDOs) defining and evolving needed standards may be coordinated and accelerated," the group said in its announcement.

At its core, a metaverse is code: ones and zeros, overlaid with unfathomably vast amounts of data. In such a world, everything comes from code. From the clothes our avatars wear to the car that we drive in, our "things" can only exist in the metaverse after being coded.

Khronos, one of the groups promoting standards behind the MSF hopes that MSF's standards will make much of that data as easily interoperable as JPEG is today. This is particularly relevant in relation to 3D objects for which no Standard currently applies.

The creation of the MSF – just a year after we first published this guide – highlights the importance of interoperable, nonproprietary data exchange formats and can result in a fundamental shift with how we interact with the internet.

In a moment where the mere idea of proprietary technology is being challenged by the advent of web3, all eyes are turning to the architects of the metaverse as the decisions they will make in the forthcoming months will likely impact IP rights for years to come.

Copyrights

Copyrights and their use in the metaverse

Beyond software, copyright protection extends to "original works of authorship fixed in any tangible medium of expression." As is evidenced by the colorful and content-full metaverses developed by Decentraland, The Sandbox or Second Life, there is seemingly no rock in the metaverse under which no copyright exists.

Collaboration and decentralization

There are many different aspects of the metaverse that will be impacted by copyright laws and this guide already touches on a number of them (see section on *Artificial intellegence* and on *Games* etc.). One aspect however deserves special attention as it is probably one of most significant challenges that we see emerging from the adoption of web3. It lies in shifting from a world of centralized and controlled servers to a decentralized internet, where content is hosted using peer-to-peer technology, like IPFS links and traded by online intermediaries, hosting other people's content. Rare are the rightsholders in music and film having worked through the nineties who won't shiver at the thought of all the effort, money and time invested in shutting down peer-to-peer platforms like Grokster, Kasaa, Limewire or The Pirate Bay. Assuming that blockchain, a technology that does not (yet) allow the storage of content, will cure the internet and vaccinate it against new copyright challenges would be naïve and short-sighted. The capacity of copyright to adapt and survive technological revolutions has been demonstrated time and time again, yet for all its transformations it has always been used to enforce a rightholder's monopoly. How copyright will fare in a world governed by DAOs and decentralized storage is anyone's guess but certainly something that we will be watching closely.

Trademarks

Trademarks and their use in the metaverse

A trademark is a word, phrase, slogan, design, or logo that operates as an indicator of source for goods or services. Trademark law protects against the unauthorized third-party use of a trademark in a manner that may dilute or disparage the trademark or in a manner that would cause a reasonable consumer to believe that the trademark owner either was the source of the goods or services or endorsed or sponsored such goods or services.

Trademarks are important features in the virtual landscape, and their use is prevalent in the metaverse. As people and companies continue to create and establish their presence online and in the world of virtual and augmented reality, this presents both opportunities and risks. Trademark owners who successfully leverage the metaverse to engage in cross-promotional branding can reach a wider audience, but they must be aware of the potential liability associated with that expanded reach.

Issues for owners and users of trademarks in the metaverse

While mixed and augmented reality have allowed brand owners to extend their reach to a growing new industry and consumer base, they have also created issues for both owners and users of trademarks, particularly in the gaming space. For example, a common issue with the intersection of the virtual and real worlds has been the use of real-world, third-party trademarks in video games that simulate the real world.

In the United States at least, trademark owners have not always fared well in their efforts to enforce trademarks used in virtual worlds. An early example of the potential pitfalls of using real-world trademarks in the virtual world played out in the case of *E.S.S. Entertainment 2000, Inc. v. Rock Star Videos, Inc.*, 547 F.3d 1095 (9th Cir. 2008). In E.S.S., the issue was whether a virtual depiction of a real-world strip club in the popular game Grand Theft Auto: San Andreas infringed the real strip club's logo and

exterior design trademark rights. The court ultimately held that the depiction of the strip club in the video game did not infringe the strip club owner's trademark and trade dress rights as the video game was an artistic expression protected by the First Amendment, and it was unlikely that consumers would be confused into believing that the strip club produced the sophisticated video game.

With the proliferation of user-generated content in the last few decades, as well as online "virtual world" games such as Pokémon Go, The Sims, and Second Life, a new set of issues has arisen involving the use of third-party trademarks in virtual worlds. For example, Second Life, a large multiplayer role-playing game that also operates as an online economy, allows users to create their own virtual worlds, develop and promote intellectual property, and even sell their own branded creations (or those of others – more on that below) for a profit. Users can even build an online business presence in Second Life to sell their products in the real world. Beauty and fashion brands can also engage in the metaverse by allowing avatars (virtual characters created by real users/players) to try on clothing or cosmetics or wear an article of clothing that real users or players may not be able to afford in real life. However, with these opportunities also come the risks of unauthorized use of third-party trademarks and possible brand dilution. For example, avatars can sell and purchase virtual goods bearing the trademarks of third parties. Thus, trademark owners should also be aware of the risks presented with the use of brands in these "virtual worlds." While case law surrounding the use of trademarks in the virtual space is unsettled and still developing, some issues that have arisen in recent cases include:

- *Nike, Inc. v. StockX LLC*, No. 1:22-cv-00983-VEC (S.D.N.Y. July 14, 2022): In this case, Nike alleges that StockX – the operator of an online resale platform for various brands of sneakers, apparel, luxury handbags, electronics, and other collectible goods – is "minting" digital assets or non-fungible tokens (NFTs) that prominently use Nike's trademarks. Nike further alleges that StockX is "marketing those NFTs using Nike's goodwill and selling those NFTs at heavily inflated prices to unsuspecting consumers who believe or are likely to believe that those "investible digital assets" (as StockX calls them) are, in fact, authorized by Nike when they are not." Nike alleges claims for trademark infringement, trademark dilution, and several other related claims in this closely watched case that is still in its early stages at the time of writing.
- *Hermès v. Mason Rothschild*, 22-CV-384 (JSR) (S.D.N.Y. May. 18, 2022): In this case, the plaintiff – the fashion house Hermès – sued Mason Rothschild (an NFT creator) for trademark infringement as a result of NFTs created by Rothschild. Specifically, Rothschild created a virtual series of purses, coined "MetaBirkins," in a series of NFT images that depicted Hermès' BIRKIN bag design covered in various furs. Hermès' complaint, which was filed in January 2022, asserted that the MetaBirkin NFTs infringed upon and diluted its registered BIRKIN trademarks, as well as its trade dress rights in the BIRKIN bag form. Rothschild submitted a motion to dismiss in February 2022, arguing that the MetaBirkins are works of art that provide commentary on "animal cruelty" and that the NFTs "are not handbags." In May 2022, the Southern District of New York rejected this motion to dismiss and allowed the case to move forward, concluding that Hermès had made sufficient factual allegations to support a conclusion of explicit misleadingness and bad faith.

- *Pellegrino v. Epic Games, Inc.*, No. 19-1806 (E.D. Pa. Mar. 31, 2020): In this case, the plaintiff – a saxophonist who went viral on the internet for his dance moves – sued the developer of the popular video game Fortnite, alleging that the game featured a virtual saxophone-playing avatar that copied his dance moves. The court dismissed Pellegrino's claim for violation of his right of publicity based on the First Amendment. The court also dismissed Pellegrino's trademark claim, finding the allegations were better suited for copyright law. The court allowed Pellegrino's claim for false endorsement to proceed, but after the court issued its order, Pellegrino withdrew his case.
- *AM General LLC v. Activision Blizzard, Inc*., No. 17-cv-8644, slip op. 11 (S.D.N.Y. Mar. 31, 2020): In this case, AM General, the company behind the Humvee truck, sued Activision Blizzard, alleging trademark infringement for including the truck in Activision's Call of Duty video game. The court found for Activision Blizzard on summary judgment under the First Amendment, explaining that (1) "Defendants' uses of Humvees in Call of Duty games have artistic relevance," and that (2) "[f]eaturing actual vehicles used by military operations around the world in video games about simulated modern warfare surely evokes a sense of realism and lifelikeness."

These cases establish that the risks of liability for a user of a third-party trademark are greater when the unauthorized user is engaging in commercial activity using the trademark. But certainly, questions of dilution and disparagement will become more prevalent themes as beauty and fashion brands continue to be immersed in the metaverse.

Best practices for trademark owners

As the metaverse continues to grow and evolve, and the lines between the real world and the virtual world continue to blur, brand owners may need to enforce their trademarks not only in the real world but also in the virtual world. Below are steps that brand owners should consider to protect their valuable trademarks.

- Register the trademark. Brand owners are strongly encouraged to register their trademarks with the U.S. Patent and Trademark Office (USPTO) and foreign equivalents. In the United States, doing so creates a rebuttable presumption that the owner owns the exclusive right to use its trademark in connection with its goods or services, and it puts the owner in a much better position to rebut any unauthorized use of its mark in either the virtual world or the real world.
- Consider subscribing to a trademark watch service. It is impossible for a trademark owner to monitor and track every infringing use in the market, especially when the owner has a large trademark portfolio. As such, trademark watch services can assist trademark owners in monitoring relevant markets and internet content for possible infringing activity. Consider designating outside counsel to review these reports as they come in. By working with a watch service, owners can be notified of infringing activity sooner rather than later and can take swift action as these issues arise.
- Immediately notify the platform of infringing activity. Assuming the infringing activity is being conducted by a third-party platform user, brand owners should report this infringement to the platform. Many of these entities do not want to be liable for any contributory infringement and will have mechanisms in place to remove the infringing content when they become aware of it.

- Evaluate the nature of use and the possible claim. Once aware of possible infringing activity, consider the nature of the infringing use and how such use affects the overall brand and the market for the goods or services associated with the brand. As illustrated in the above case examples, not all trademark use in the metaverse is actionable. Outside counsel can assist with this analysis and can help to determine what obstacles, if any, may exist to the enforcement of the trademark. It is also important to note that in the United States, brand owners of nationally known brands are in a better position to enforce against unauthorized use since under the Federal Trademark Anti-Dilution Act, owners of nationally recognized or "famous" brands can sue if the unauthorized use of their trademark by others "tarnishes" or "blurs" the trademark. The Act applies regardless of whether consumers are confused as to the source of the goods.
- Establish a metaverse presence. Finally, brand owners should consider establishing a metaverse presence of their own. Aside from the benefits that come with leveraging the metaverse as an alternate means of reaching consumers and building brand awareness via a thriving and growing market, having a metaverse presence also provides an opportunity to monitor activity, and it may even help thwart trademark infringement by bad-faith actors.

Patents

Patents and their expanding use in the metaverse

A patent for an invention is the grant of a property right to the inventor, issued by USPTO. Generally, the term of a new patent is 20 years from the date on which the application for the patent is filed in the United States or, in special cases, from the date an earlier related application was filed, subject to the payment of maintenance fees. U.S. patent grants are effective only within the United States, U.S. territories, and U.S. possessions. Under certain circumstances, patent term extensions or adjustments may be available.

Companies developing metaverse-related technologies often use patents to protect their inventions. Most metaverse-related patents are in either the VR or AR space. The number of new patents filed related to AR/VR has increased globally at an annual rate of 33 percent since 2010. This exponential rise in the number of filings indicates the increased research and development spending on metaverse-related inventions.

That observation is accurate both with regard to the United States and Europe. The widespread myth according to which software solutions are not patent eligible in Europe is, in fact, wrong. Provided that an invention is computer-implemented, the subject matter may potentially be patented. Statistics show that every fourth patent application with the European Patent Office relates to a computer-related invention.

Additionally, research on and development of metaverse-related inventions are no longer restricted to entertainment and science fiction. AR/VR-related patents are now being used in a wide variety of industries, such as online shopping, workplace training, health care delivery, and real estate.

Issues for owners and users of patented inventions in the metaverse

As with other intellectual property, patent use in the metaverse presents opportunities and risks. A particularly lucrative benefit of owning a patent focused on AR/VR technology is potential licensing revenue. However, identifying potential licensees may present a challenge. In fact, owners of patented inventions used in the metaverse face even greater challenges in policing infringement than do owners of copyrights and trademarks. That is because the use of a software patent is not always visible in the metaverse. Indeed, proof of infringement of a software patent such as an AR/VR patent often turns on the analysis of source code, which is not available until the patent owner has filed a lawsuit and obtained the source code during discovery.

The risks to owners of metaverse-focused patents include potential invalidation of the patents during litigation to enforce the patent. U.S. courts increasingly have been invalidating software-focused patents as "abstract" and ineligible for patenting under section 101 of the U.S. Patent Code and also under the landmark U.S. Supreme Court decision in *Alice Corp. v. CLS Bank International*, 573 U.S. 208 (2014). The law in this area is still developing and is murky at best. On June 30, 2022, the United States Supreme Court declined the opportunity to clarify the law in the closely watched case, *American Axle & Manufacturing v. Neapco Holdings LLC*. In that case, a fractured Federal Circuit (the U.S. appellate court dedicated to patent-focused appeals) found that patent claims for reducing vibration in automotive propeller shafts were patent ineligible under 35 U.S.C. section 101. The Supreme Court's next term will present another opportunity for clarifying the law on patent eligibility – this time in connection with a metaverse-focused patent. Specifically, in *Worlds Inc. v. Activision Blizzard Inc.*, the Court will decide whether or not to weigh in on a decision invalidating a patent claiming a method of avatar crowd control in a virtual space, based on filtering avatar positioning information. In the meantime, the continued uncertainty in this area of the law creates uncertainty in the value of patented AR/VR inventions.

Best practices for owners of metaverse-related inventions

Because of the uncertainty surrounding patent eligibility for software inventions in the United States, owners of such inventions might consider not filing a patent at all, and instead protecting the invention as a trade secret. Furthermore, depending on the subject matter of an invention (for example, a process-related one), it may be preferable to opt for trade secret protection because patent enforcement against a competitor would prove to be difficult. Every invention starts as a secret. At some point, the inventors (or the owners of the invention) have to choose whether to keep their invention a secret or to file for patent protection. Keeping a software invention a trade secret avoids having to prove that the invention is not merely an "abstract idea" and that it is therefore eligible for patenting. In determining whether to patent a software invention or instead to treat it as a trade secret, the owner of the invention should consider:

- Whether the invention will be useful for more than 20 years. If so, it is worth exploring trade secret protection because trade secrets can last longer than the 20-year life of a patent, assuming the trade secret does not become stale due to advances in technology.
- How difficult it is for other companies to reverse engineer the invention. The easier it is to reverse engineer an invention, the less likely it will be to consider it a trade secret.
- How often their employees who have access to the invention change jobs. It becomes more difficult to protect trade secrets in industries with high turnover rates and in jurisdictions that do not view non-compete restrictions favorably.

The good news is that thanks to the EU Trade Secrets Directive, the level of protection afforded to trade secrets has significantly improved. Indeed, standards in the United States and Europe are converging.

Domain names

After some initial hiccups, the World Wide Web's domain name system has organized itself under ICANN with a finite number of Top Level Domains (TLDs) and has provided avenues for brand owners to defend their online turf with the Uniform Dispute Resolution Policy (UDRP). Web3 and the metaverse threaten to turn back that advancement. NFT-based domains using a new set of TLDs, independent from ICANN and the UDRP and operating on a registrar-free smart contract, will possibly bring us back to the dot-com era of domain name gold rushes. This means that for now, trademark and brand owners need to be proactive and consider registering the crypto and metaverse versions of their brand names as domain names. The blockchain-based domains often have decentralized governance models and atypical registration terms. These have to be carefully considered and understood, but it means that the old rules do not apply. In addition, it would be advisable to also register the new trademarks as a defensive measure to future domain name disputes.

Open source

The open-source movement rose to prominence in the web1 dot-com boom era. This new platform required a whole raft of tools (remember the browser wars?) in order to tap its full potential. Open source provided some of the answers with its online distribution model. In web2, the walled garden of social media giants meant that content, eyeballs, views, and followers were key performance indicators to the proprietary tools needed to run web2, and open-source software took a backseat. Web3 might herald back the open-source era – the decentralized applications are developed on open-source software and protocols and users can interact with each other through interoperable metaverse properties. The real value in the metaverse lies in the user interactions and the user data, and the fight will be over the ownership of these properties. The applications and software will not take a back seat this time; the data will be on the blockchain. Going open source will encourage the metaverse to be as open and interoperable as possible while leaving the monetization efforts to other features of distributed ledger technology. All the issues relating to jurisdiction and intellectual property with regard to the metaverse apply to open source as it is primarily based on copyright law, which is a jurisdiction-dependent statutory matter.

These choices are strategic and require owners of AR/VR and other metaverse-related inventions to think about the broader picture of intellectual property ownership and its associated benefits and risks.

Authors

Sohie Goossens
Partner
London
sgoossens@reedsmith.com

Dr. Anette Gärtner LL.M.
Partner
Frankfurt
agaertner@reedsmith.com

Christine Morgan
Partner
San Francisco
cmorgan@reedsmith.com

Bryan Tan
Partner
Singapore
bryan.tan@reedsmith.com

Fred Ji
Associate
San Francisco
fji@reedsmith.com

Sarah Bruno
Partner
San Francisco
sbruno@reedsmith.com

Investing in the metaverse

While the blockchain markets – alongside many other global markets – experienced broad downturns in the first half of 2022, this has not deterred founders and investors in the industry, who continue to see the long-term prospects for the technology and so have maintained a tremendous level of interest in building new projects in the space, including those focused on the metaverse.

Prior to the downturn, 2021 saw a range of big-ticket crypto M&A announcements, highlighted by Galaxy Digital's $1.2 billion purchase of digital-asset custodian BigGo, as well as deals like Mastercard's foray into the industry with the acquisition of crypto intelligence firm CipherTrace, Nike's purchase of NFT development and production house RTFKT, and a wide variety of other major transactions.

Reports indicate that we can expect 2022 to continue to be an extremely active time for investment in the space. According to PwC, the total amount raised by companies in the crypto industry in 2021 was almost eight times higher than it was in 2020, reaching a total of $34 billion, which was more than all prior years combined. Early indications are that 2022 may yet outpace that record year, with capital inflows from crypto VC firms topping $14.6 billion in the first quarter, which is equal to about 48 percent of the total raised in all of 2021.

With big institutional investors such as a16z and FTX raising new multibillion-dollar funds in 2021, and other familiar names, including Sequoia and Bain Capital, taking in hundreds of millions of dollars of their own, investment interest in this space can be expected to persist for years to come. Investment in the blockchain industry is no "flash in the pan," and has captured the attention of entrepreneurs and investors who wish to align to create valuable products and reap the benefits of their efforts.

Compared to conventional technology start-ups, investing in a metaverse or blockchain project can be more complex in some respects, but also more attractive in others.

The basic assumption for conventional tech start-up investments is that the value of the enterprise is captured through equity interests in the company that houses the project. The project founders and other key participants pool the intellectual property and other key assets relating to the project into a corporation or other legal entity, and that entity is tasked with building a business that will eventually generate profits that can be distributed to its owners. The potential for future profits to be generated by the enterprise is also captured by the share value of the entity, which is expected to appreciate as the business grows, execution risks are mitigated, and the business proposition is validated.

In this conventional start-up context, the assumption is that the value of the enterprise is mirrored 1:1 by the value of its shares. Consequently, investing in the enterprise almost always involves acquiring shares of the company that houses the project. The company sells shares to investors to raise capital to build the enterprise, and investors acquire shares on the assumption that the shares will appreciate in value if the venture is successful. Investors expect to make a return on investment through receiving a share of profit distributions – or, more importantly, by selling their shares at a profit at a later point. The opportunity to sell is expected to come through a sale of the company, through an IPO or exchange listing that generates a public market for the shares, or through private secondary sales.

Equity interests in a conventional technology enterprise also play another important role – they facilitate governance mechanisms to ensure that the interests of the external stakeholders in the enterprise are adequately protected. Investors in tech companies will often participate in governance of the enterprise through rights to vote on and approve key events – such as a sale of assets or additional financing transactions – and rights to elect company directors to directly oversee its management. These governance functions are enabled through voting rights attached to the shares investors hold.

In the context of a metaverse project, however, some of the base assumptions for traditional venture investments may not be present. For one thing, the declared goal of many blockchain projects is not to create a profit-making enterprise. On the contrary, web3 projects are often designed to avoid a result where the originators of the project profit at the expense of the community that eventually adopts and uses the platform to be developed. Instead, the professed motive is often to build an infrastructure that generates benefits shared equally among the community. Therefore, there may not be a stream of expected future profits to be captured by shares of the legal entity that originates the project. Moreover, the likelihood of an "exit event" generating liquidity for holders of these shares may be questionable. Outright acquisitions of web3 companies have – to date at least – been comparatively rare. And public offerings and exchange listings of equity interests in the blockchain projects have been rarer still.

For investors, holding shares in the company they invest in may not afford much assurance of involvement in governance matters either. In part, this is due to the fact that the legal entity that accepts investor capital may not be the entity that ultimately launches and operates the project – many blockchain projects evolve to operate under the auspices of multiple legal entities, often spread across several legal jurisdictions. Moreover, many projects aim to ultimately place much of the authority for steering the project in the hands of their user community through decentralized governance processes.

All of this may make investing in a metaverse start-up seem like a daunting proposition. However, the flip side is that web3 projects may offer investors paths to liquidity not present with conventional venture investments.

That's because these projects often entail building an economy around tradeable digital assets created by the project. A central mechanism of metaverse or other blockchain projects is often one or more digital "tokens" that enable access to features, functions, and services offered by the platform, or, in some cases, digital currencies that act as a medium of exchange within the online economy enabled by the project. For instance, a digital virtual world project may employ a token to enable users to vote on referenda about the evolution of the online platform, or to access tools to build their presence within the online universe. The project may also support a digital currency that enables actors in the digital universe to exchange goods or services within the online realm.

These digital assets are often designed to be transferable and tradeable, whether within a trading system operated by the project itself, or on a variety of third-party digital asset exchanges (including popular "centralized" asset exchanges such as Coinbase, Binance, and FTX, as well as smart-contract-based "decentralized" exchanges such as Uniswap and Sushi).

These digital assets also typically serve as a mechanism for incentivizing the teams of developers that create and support the project, including the founders that originated it, by allocating certain of these tokens or coins to these key players. And, importantly, such digital assets can serve as a mechanism for rewarding early investors in the project for their support. A common practice for web3 projects is to devise a digital asset economy with a limited supply of digital assets (to support a sustainable long-term value for these assets), with a defined portion of the available supply allocated to rewarding and incentivizing different constituencies supporting the project, including investors that helped underwrite the cost of developing and launching the project.

This means that investors supporting a web3 project may be able to count on access to a class of digital assets that are liquid and act as a proxy for the overall value of the project the investors supported. As a result, investors in these projects are often not solely reliant on the equity interests they purchased to realize liquidity. Multiple paths to liquidity may be available if investors hold both equity in the legal entity that originated the project and the digital assets that the project produces. Indeed, some of these paths may offer a much shorter time horizon to liquidity than traditional venture investments – whereas the timeline for exiting an early-stage equity investment through an M&A transaction or public stock offering is measured in years, if not a decade or more, a liquid market for digital assets of a web3 venture could emerge within a year or less of the project raising initial external funding.

The key consideration for investors in blockchain start-ups is therefore often to ensure that they are positioned to participate in all potential sources of value – including ownership not only in the legal entities they support but also in the digital asset economies the projects aim to create.

Once the parties have aligned on structure, the question of valuation becomes important. While the valuation of traditional start-ups is often difficult, the valuation of metaverse and other blockchain start-ups is even trickier. For one, there are few established comparators to use as benchmarks with respect to a newly proposed deal (and even fewer that are public), particularly in the metaverse space. Further, the technology underlying these projects is still evolving and many metrics, such as daily active users, are estimates, lending even more uncertainty to the medium- and long-term forecasts of a particular investment's value. Using a discounted cash flow analysis is also difficult, as the token structures used by many metaverse and other blockchain start-ups effectively amount to indirect and non-regular income streams, and thus do not cleanly align with this kind of conventional modeling. In addition, the uncertainty over the ownership of data and intellectual property in the metaverse casts doubt over key factors traditionally used to value start-ups.

Beyond the structuring of the deal itself, investors conducting their due diligence in the blockchain space must be mindful of the unique regulatory compliance issues affecting the industry, as compared to traditional venture capital deals.

Often, the most prevalent and pressing compliance concerns for a crypto project relate to the potential classification of its associated digital assets as securities under the laws of the United States and other jurisdictions. In the past, the U.S. Securities and Exchange Commission (SEC) has provided rough guidelines regarding its thinking around which digital assets may be deemed to be securities. However, even if these guidelines are taken to still represent the SEC's working framework (which is not guaranteed, given the recent changes in regulators heading the SEC and other agencies), such guidelines are incredibly complex and nuanced – there are around 40 factors that must be evaluated and weighed against each other regarding any given digital asset, just to glean a rough probability on how the SEC may land regarding such an asset's securities status.

Classification of a project's digital assets as securities could have substantial negative implications for the value of the assets and, therefore, for an investor's investment in the project. Digital assets that are deemed to be securities may have far fewer options regarding centralized exchanges that are willing to list the asset, thus limiting the market liquidity for the asset. And the assets would likely be subject to restrictions on transfer for considerable periods of time, even further impacting the assets' salability and the enterprise's commercial viability. Depending on the degree to which a project operates in a decentralized manner, certain reporting requirements imposed by current securities laws could even be impossible for the project to comply with.

Beyond the complicated analyses that must be conducted regarding federal securities laws, certain crypto projects could also implicate several other U.S. legal, regulatory, and monetary regimes, overseen by agencies such as the Commodities Futures Trading Commission (CFTC), the Financial Crimes Enforcement Network (FinCen), the Internal Revenue Service (IRS), the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board, the Federal Deposit Insurance Corporation (FDIC), the Department of Justice (DOJ) and any number of other international and state-level oversight bodies. Investors must also bear in mind that many web3 projects are designed in ways that are not limited geographically, and as such, their compliance obligations are inherently global. The fact that the regulatory framework for digital assets is largely unsettled – both within and beyond the borders of the United States – presents unique challenges and risks for industry participants beyond those faced by most conventional start-ups.

In summary, while differences between investment in conventional start-ups and in metaverse or other blockchain projects may deter some would-be participants, it is clear that these novel risks and considerations have not deterred a large class of investors from entering the industry. Those seeking to join in on the excitement in this space should do so with clear eyes and an understanding of how best to structure crypto-related projects and avoid regulatory pitfalls associated therewith.

Authors

Ramsay Hanna
Partner
Century City
rhanna@reedsmith.com

Bryan Tan
Partner
Singapore
bryan.tan@reedsmith.com

Evan Zinaman
Associate
Century City
ezinaman@reedsmith.com

Artificial intelligence

In 2018, a painting created using artificial intelligence (AI), "Portrait of Edmond de Belamy," was sold at a Christie's auction for $432,500, while AI start-up JukeDeck composed music sung at a K-pop concert in Seoul. In 2016, Flow Machines – an AI system developed by SONY CSL Research Lab – composed new music based on everything from the Beatles to Bach. Veritone, a leader in enterprise AI software, recently partnered with the estate of Walter Cronkite to create a synthetic voice model of the iconic American broadcast journalist. Craiyon's AI text-to-image generator, which is publicly available, draws art based on word prompts.

"Portrait of Edmond de Belamy" by Paris-based arts-collective Obvious

Advances in technology, the development of the metaverse(s), and the expectations of today's consumers continue to propel the demand for next-level content. The considerable cost of producing high-quality, ultra-realistic artwork at a faster rate is a harsh reality for creators across many industries, including games, film, television, automotive, architecture and more. The finite amount of creators and time available to design adds another layer of challenges and causes an increasing number of industries to turn to AI assisted artistry to solve the problem of producing and scaling high-quality content.

Introduction

AI uses machine learning technologies to review, digest, and analyze vast quantities of data to create rules of application called algorithms. Once "trained," machine learning software can continually improve itself through the analysis of new data sources and through the observation of its own data output. In recent years, AI has expanded to include computing systems that aim to replicate the function of the human brain in analyzing and processing information (called artificial neural networks), as well as pairing computer networks in generative adversarial networks where the computers learn from each other.

The massive ingestion of data by AI machines and the works they create have generated considerable debate in the legal world, from which two key questions have emerged:

1. Can AI digest massive databases that include works protected by copyright and use machine learning to "author" creative works without infringing on copyright?

2. Is the output generated by an AI system protectable under copyright laws?

Another area of increasing scrutiny in the sphere of machine learning and AI is that of ethical compliance of AI systems – as evidenced by the increasing number of academic papers and debates occurring in that space.

Training AI with data protected by copyright

Generating works using AI is a creative process that often differs from traditional computer-generation. With the latest types of AI, the computer program can make many of the decisions involved in the creative process without human intervention, thereby elevating it from the status of "tool" to that of "creator." At European policy level, considerable thought is currently being given to this particular question of AI-generated creations, as indicated in particular by the European Commission in its Communication of November 25, 2020.[1]

Separately, policy-makers continue to debate questions arising from the use of data that is protected by copyright for machine learning purposes, during the stage leading to the development of software capable of self-generating "creations."

Data and information used to train an AI system may or may not be subject to restrictions. Not all information is "protected" or "owned" – for example, protection is unlikely to extend to historical information about weather patterns, pollution levels, the shape of clouds, satellite imagery or birdsongs.

What about content protected by copyright? In any text and data mining ("TDM") process it is typically necessary to "clean" the text and data being mined (which in some cases takes up to 80 percent of the mining time), in order to remove inconsistent, unreliable or redundant data, and to "normalize" the data into a specific format adapted to the relevant application. These mining operations usually involve copyright issues because they involve upstream acts of reproduction of the works or databases concerned. In order to be "read" by an AI system, they must be stored, at least temporarily, and sometimes modified (e.g., by formatting, cutting, merging, compilation, etc.) to make them usable. Each of these copying operations is likely to engage the right of reproduction that is reserved to the relevant copyright owners, which requires the express authorization of

1 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Making the most of the EU's innovative potential – an intellectual property action plan to support the EU's recovery and resilience, 25 November 2020, available here.

those copyright owners for the exercise of those rights. In the same vein, the storage and, if necessary, the communication of copies of the initial data set to third parties without such authorization is likely to infringe the monopoly rights of those copyright owners, unless an applicable exception exists. One of the most frequently used exceptions, under U.S. law, is the doctrine of fair use. However, the U.S. law approach differs considerably in that respect from the approach adopted recently under EU law, at articles 4 and 5 of the Copyright Directive (2019-790).

The differing, patchwork approaches of different jurisdictions to TDM exceptions creates opportunities for arbitrage of national copyright laws when it comes to carrying out TDM, particularly for commercial purposes. The absence of an untrammeled TDM exception within the EU clearly has potential to encourage AI users to train their AI systems on data placed on servers in jurisdictions with clear copyright exceptions, and to create consequential effects in areas such as business structuring, investment decisions and talent retention.

Text and data mining in the United States

As AI search engines crawl through the World Wide Web endlessly seeking, digesting, and aggregating content, they inevitably digest copyrighted works such as music videos, songs, novels, and news stories. Since this digestion – which generally requires the making of a copy – is frequently performed without the express consent of the copyright holder, its legality often depends on whether it is permitted under an exception to, or outside the framework of, copyright law. Under U.S. copyright law, the exception that is most frequently relied upon is "fair use."

Under section 107 of the Copyright Act, "fair use" is a four-factor test: (1) the purpose of and character of the use; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the whole; and (4) the effect of the use on the potential market for, or value of, the copyrighted work. Fair use of a copyrighted work for such things as teaching, scholarship, and research is specifically permitted by section 107. A key consideration that courts have used in deciding whether fair use exists is whether the use is "transformative."

Whether copying of copyrighted material for the purpose of machine learning constitutes fair use is a hotly debated topic that will affect the future of AI in the United States. For example, Thomson Reuters and West Publishing Corp. have sued Ross Intelligence, Inc. over, among other things, its alleged use of machine learning to create a legal research platform for Ross from the Westlaw database. The outcome of this case is still pending, although Ross' motion to dismiss was denied.[2]

Will fair use protect machine learning?

In a seminal case from 2015, the Second Circuit found Google Books' scanning of more than 20 million books, many of which were subject to copyright, to be a non-expressive" and transformative fair use of the texts because Google Books enabled users to find information about copyrighted books, as opposed to the expressions contained in the books themselves.[3] A key learning from the case was the distinction made between "expressive" and "non-expressive" use of copyrighted materials, the latter being deemed fair use by the court. Applied to AI, could the solution mean that so long as the original text does not "express" in the final work product, the act of machine reading is fair use?

We are not aware of U.S. courts applying fair use in the context of TDM, in part because cases considering AI functionality have often involved the express use of copyrighted material that qualified as traditional copyright infringement. For example, the Second Circuit found in a 2018 case, that although TVEyes' "search feature" for Fox News content in and of itself might have been

2 Thomson Reuters Enter. Ctr. GmbH v. ROSS Intelligence Inc., 529 F. Supp. 3d 303 (D. Del., Mar. 29, 2021).

3 Authors Guild, Inc. v. Google Inc., 804 F.3d 202 (2d Cir. 2015).

sufficiently transformative to be fair use, the fact that TVEyes also had a "watch feature" that redistributed copyrighted Fox News content to TVEyes users for a monthly fee did not permit a fair use defense (*Fox News Network, LLC v. TVEyes, Inc.*, No. 15-3885 (Feb. 27, 2018)).

In practice, major TDM search projects are generally dealt with under contract, which has resulted in low instances of litigation. Academic and commercial arguments have also been raised against over-reliance on "fair use" for TDM. As a practical matter, a key factor that U.S. courts will look at is whether TDM deprives the copyright owner of the value of their copyrighted material.

Text and data mining in the European Union (Directive 2019/790)

In Europe, the recent Copyright Directive adopted in 2019 created two TDM-specific exceptions.

1. TDM for research that focuses on TDM by research organizations and cultural heritage institutions, limited to the purposes of scientific research (art 4).
2. TDM for any purpose that applies for everyone else, but with a significant caveat: the ability for copyright holders to opt out of that exception (art 5).

The caveat allowing rights owners to opt out is significant, and could potentially place a considerable burden on the shoulders of businesses that would arguably need to verify, each time a training set needs to be copied, whether owners of the underlying copyright-protected material have opted out or not. Otherwise, businesses could inadvertently be infringing copyright.

Given that there is no incentive for rights owners not to reserve their rights, we suspect that a great number of (traditional) copyright owners will want to reserve their rights and "opt out." With regard to the manner in which rights owners could exercise their opt out, the Directive is somewhat unclear. It explains that a rights owner may only reserve those rights by the use of machine-readable means, and should be able to apply measures (e.g., technical measures) to ensure that their reservations in this regard are respected. This raises significant questions such as: (1) the exact manner in which the opt-out must be expressed; (2) at what point the TDM user needs to check whether the opt-out has been exercised (e.g., at the time when it first accesses the data, or on a continual basis?); (3) who bears the burden of proof as between the rights owner and the user (bearing in mind the difficulty a user will have in "proving a negative," i.e., that the opt-out right has not been exercised); or (4) how to determine the period of permitted retention.

Assuming that certain types of rights owners will largely seek to exercise their opt-out rights, these new TDM exceptions are likely to provide a contrasting level of protection to businesses, depending on the type of data they use. If the data being used is likely to belong to the most traditional areas of the entertainment industry, then these exceptions may provide little support for use in commercial AI applications. The geopolitical context thereby created is one in which other jurisdictions have positioned themselves favorably in the race to become global centers for TDM and AI development, through their more developed, fit for purpose copyright exceptions.

Is AI-created content copyrightable?

AI creations are certain to constitute large parts of the landscape of the metaverse's virtual worlds – sometimes literally, as in the case of the Azure-driven location models and maps generated in Microsoft Flight Simulator. The questions of rights and ownership in the outputs of AI systems raise their own problems.

International law espouses the human-centric concepts of personal expression, authorship, and originality as prerequisites for the existence of copyright in a creative work (and therefore for its protection and "ownership").

Those concepts break down when the link between a human author and the creative work is interrupted – most infamously in the "monkey selfie" case, where a photograph taken by a monkey was found not to enjoy copyright protection.[4] Outputs generated purely by AI systems (which are, depending on the facts, distinguishable from works created by humans with AI

4 Naruto v. Slater, 888 F.3d 418, 426 (9th Cir. 2018).

“In the future, making the metaverse a safe place for all is likely to require that every AI-generated three-dimensional gaming environment is devoid of biases, bullying, and other man-made expression of violence.”


BETA : 7648 34 55
ALPHA : 973 86 90 56
TD : 3765 5355 5
SCORE : 3 7 8 4 0 6 6
CONTROL ANALYSIS
1239 98239 8238
SP VM BA DA

assistance) challenge the norms that only contemplate human creation of copyright works. Even the UK's unique provision governing "computer-generated works," – where the person "by whom the arrangements necessary for the creation of the work are undertaken" is deemed the author – confirms the need to identify a human rather than a system as the author of a "creation."

Likewise, traditional justifications for copyright protection, such as incentivizing creation of works or protecting the natural rights of creators, break down when the creator is a machine requiring no incentivization and having no personality.

In short, both the EU and the UK legal systems do not appear to welcome or accommodate creations by robots, which (currently) seem destined to fall into the category of information that is free and free-flowing. Could an AI-generated metaverse reset our world by providing a great space for the public domain and "commons" to thrive?

Will an AI-generated metaverse compete with human-generated worlds in a great clash of intellectual property battles? The android's doodle of an electric sheep may have no author and no copyright protection, but the programmer of the android may still want to license it to you.

In the United States, the primary purpose of copyright law is to promote the production of creative works by providing an economic incentive to authors through the protection of their works. This economic incentive is provided to authors for the public good, because enabling authors to be rewarded monetarily for their works will lead to the production of more creative content. As AI companies continue to invest in the technologies necessary for the machine-based production of creative works, will they be able to enjoy the economic protections of copyright?

Section 102 of the Copyright Act requires that for a works to be copyrightable, they must be "original works of authorship fixed in any tangible medium of expression now known or later developed…" While neither the Copyright Act nor the U.S. Constitution addresses the requirement of human authorship, the courts and the Copyright Office have operated on that basis. The Copyright Office has rejected attempted registrations of works produced solely by mechanical processes, and has included the requirement of human authorship in its Compendium of Copyright Office Practices.[5]

In 2018, the Copyright Office rejected Stephen Thaler's application to copyright "A Recent Entrance to Paradise," a work generated by his AI system and listed author, the Creativity Machine, on the grounds that it "lacks the human authorship necessary to support a copyright claim." The Copyright Office also rejected Thaler's claim that AI can be an author under the work-for-hire doctrine.[6]

The view of the Copyright Office is that a work generally needs to be of human authorship in order to be copyrightable, with the computer merely being an assisting instrument, and where the traditional elements of authorship (such as literary, artistic or musical expression) were conceived and executed by a human.[7] This means that AI-created works in the United States will likely become part of the public domain when created and can be freely distributed. As it stands, this has profound implications for the development of AI-created works because the companies and investors behind the machines that produce them at present are not afforded protection under U.S. copyright law. There has been a lot of discussion as to whether U.S. copyright will evolve to afford this protection.

One argument for extending copyright protection to non-human authors is that other non-natural persons have been extended legal rights. Corporations in the United States have long been afforded the right to enter into contracts and enforce contracts to the same extent as human beings, as well as the obligation to pay taxes.

Some commentators have argued that the end user of an AI program generating creative content should be the owner of that content, using a concept of a machine-based work-for-hire doctrine, with the AI program being deemed the equivalent of a contractor who is hired by an employer to produce content owned by that employer.[8]

5 "[T]he Office will refuse to register a claim if it determines that a human being did not create the work." U.S. Copyright Office, Compendium Of U.S. Copyright Office Practices § 306 (3d ed. 2021).

6 Letter from Shira Perlmutter, U.S. Copyright Office Review Board, to Ryan Abbott, Esq. (Feb. 14, 2022) (on file with the U.S. Copyright Office).

7 U.S. Copyright Office, Compendium Of U.S. Copyright Office Practices § 313 (3d ed. 2021).

8 See Wenqing Zhao, AI Art, Machine Authorship, and Copyright Laws, 12 Am. U. Intell. Prop. Brief 1 (December 2020).

"Governments have used versions of the technology in criminal justice and the allocation of public services like income support."

Others have cited the creative contributions that the end user makes in directing the AI program to produce a creative work as a justification for the end user being deemed an author of the AI-produced content, viewing the AI program as a tool of the end user.[9]

AI as an enforcement mechanism to protect copyright

Beyond having the ability to produce creative works, machine learning also provides human authors with the ability to enforce their rights and to better monetize their rights. Companies like Audible Magic, as well as Google and YouTube, have developed AI software that recognizes content and helps detect potential copyright violations. Their technologies should yield significant economic benefits for human authors.

Is AI-created output infringing?

The fact that AI can create output that mimics human expression and personalization means that AI's use of copyrighted works for the purposes of machine learning may harm the market for works by human authors and thus come under increased scrutiny by (human) rightsholders. Even if the creation of the AI systems in and of itself is not infringing, if output generated by an AI system that has been trained on a particular type of data is substantially similar to the data in the dataset, it may be an unauthorized "derivative work" that infringes copyright in the preexisting works, which is a scenario far more likely to unfold with small and very small datasets.

Should AI copyright be based on creativity?

Some countries, such as the United Kingdom, have moved toward protecting computer-generated works (steered by humans) based on the elements of creativity contained in the work in order to encourage investment in AI systems. As AI continues to develop and generate more "creative" works, the debate over the ability to copyright these works, and who can own them, will undoubtedly grow.

Ethics

The other area of considerable interest in the sphere of machine learning and AI is that of ethical compliance of AI systems – witness the increasing number of papers and debates happening in that space.

Today, the ethical ramifications and pitfalls of AI are considered to be highly application-specific. The potential for in-built biases of the AI system to create serious consequences for human subjects is deemed much more obvious in the context of, for example, criminal justice applications than that of an AI generator of artwork. This underlies the identification by the European Commission in its recent draft AI Regulation of "high risk" AI applications, which are to be subject to statutory standards.

In the future, making the metaverse a safe place for all is likely to require that every AI-generated three-dimensional gaming environment is devoid of biases, bullying, and other man-made expressions of violence all too often experienced in our real-world environment.

When the day comes, it seems very likely to us that all AI operators – to a greater or lesser extent, depending on the nature of their applications and whether, as a matter of legal compliance or commercial best practice (for example, in adhering to voluntary sector standards and benchmarks) – will need to consider their internal processes and governance with respect to the high level of safety and security that will be required to enter the building site of the metaverse.

The scope for bias in systems and outputs; the quality and nature of training data; systems resilience and accuracy; human oversight and intervention – to name but a few factors – are likely to be necessary to ensure that humans feel comfortable, safe, and at ease in the metaverse.

9 See Nina Brown, Artificial Authors: A Case for Copyright in Computer-Generated Works, 20 Sci. & Tech. L. Rev. 1 (Fall 2019).

Europe's approach to AI and the metaverse

On April 21, 2021, the European Commission published their long-awaited proposal for a regulation on AI, aiming to turn Europe into the global hub for trustworthy AI (Proposal for a Regulation laying down harmonized rules on AI, Artificial Intelligence Act).

The EU Commission's proposal is the result of several years of preparatory work by the Commission, including the publication of a "White Paper on Artificial Intelligence." The vision of the Commission is to protect and strengthen fundamental rights of people and businesses while at the same time encouraging AI innovation across the EU.

Various EU member states have already reacted to the proposed AI Act. A decision on the proposal is intended for November 2022. However, it is not yet clear whether this timeframe can be met as there are still too many topics being heavily discussed. Moreover, it also seems that there are still some gaps in data protection law, which could be a major barrier to the Artificial Intelligence Act.

To whom does the proposal apply?

The newly proposed regulation would apply to (1) providers that place on the market or put into service AI systems, irrespective of whether those providers are established in the European Union or in a third country; (2) users of AI systems in the EU; and (3) providers and users of AI systems that are located in a third country where the output produced by the system is used in the EU.

What is in this proposal?

The Commission takes a risk-based but overall cautious approach to AI and recognizes the potential of AI and the many benefits it presents, but at the same time is extremely aware of the threats these new technologies pose to the European values and fundamental rights and principles.

They follow a risk-based approach that is essentially divided into four parts:

1. **Unacceptable risk**: AI systems that are considered as a clear threat to the safety, livelihoods, and rights of people are generally prohibited. An unacceptable risk exists especially when systems or applications manipulate human behavior to influence the user's free will, and that could lead to psychological or physical harm. For example, toys using voice assistance to encourage minors to engage in dangerous behavior would fall in this category.

2. **High risk**: AI systems identified as high risk are permitted, but subject to special requirements and conformity assessments. Such systems include AI technologies used in various areas that need higher protection, such as education, critical infrastructure, employment management, security components of products, law enforcement in cases of interference with people's fundamental rights, or asylum and border control management.

   Just to name a few special obligations: The systems must go through adequate risk assessment and mitigation systems before being placed on the market. In addition, they have to provide a high quality of data sets, a detailed documentation about all information necessary on the system, and its intended purpose so that authorities can assess compliance. The systems must meet the requirements of transparency and information for the user and must be overseen by humans to minimize risks.

In particular, all remote biometric identification systems are placed in this category and are subject to these strict requirements. Their live use in publicly accessible spaces for law enforcement purposes is generally prohibited. Very few strict exceptions are allowed, and these must be authorized by a judicial body (for instance, when absolutely necessary to search for a missing child).

3. **Limited risk**: AI systems with limited risks are generally permitted but also have to fulfill specific transparency obligations. AI systems such as chatbots shall make users aware of the fact that they are interacting with a machine so that they can make an informed decision to either continue or stop.

4. **Minimal risk**: The vast majority of AI systems, such as video games or spam filters, fall into this category and are legally allowed as there is minimal risk or no risk at all for users' rights or safety.

What's next?

The European Commission's 108-page proposal is an attempt to regulate an emerging technology before it becomes mainstream. As the European Union has been the world's most aggressive watchdog of the technology industry, it may serve as a blueprint for similar measures around the globe.

The rules have far-reaching implications for major technology companies that have poured resources into developing AI, but also for scores of other companies that use the software to develop medicine or judge creditworthiness. Governments have used versions of the technology in criminal justice and the allocation of public services like income support. The broad definition of AI systems ensures that the regulation would have a significant impact in all industry sectors, in particular in those sectors that want to have success with the metaverse.

The proposal now goes to the European Parliament and the member states in the ordinary legislative procedure. Given the controversial nature of AI and the large number of stakeholders and interests involved, it seems likely that this will not be a straightforward process. There will likely be many amendments and, hopefully, also some further clarification. Once the law is adopted and passed, the regulation would be directly applicable in all member states in the EU.

Authors

Sophie Goossens
Partner
London
sgoossens@reedsmith.com

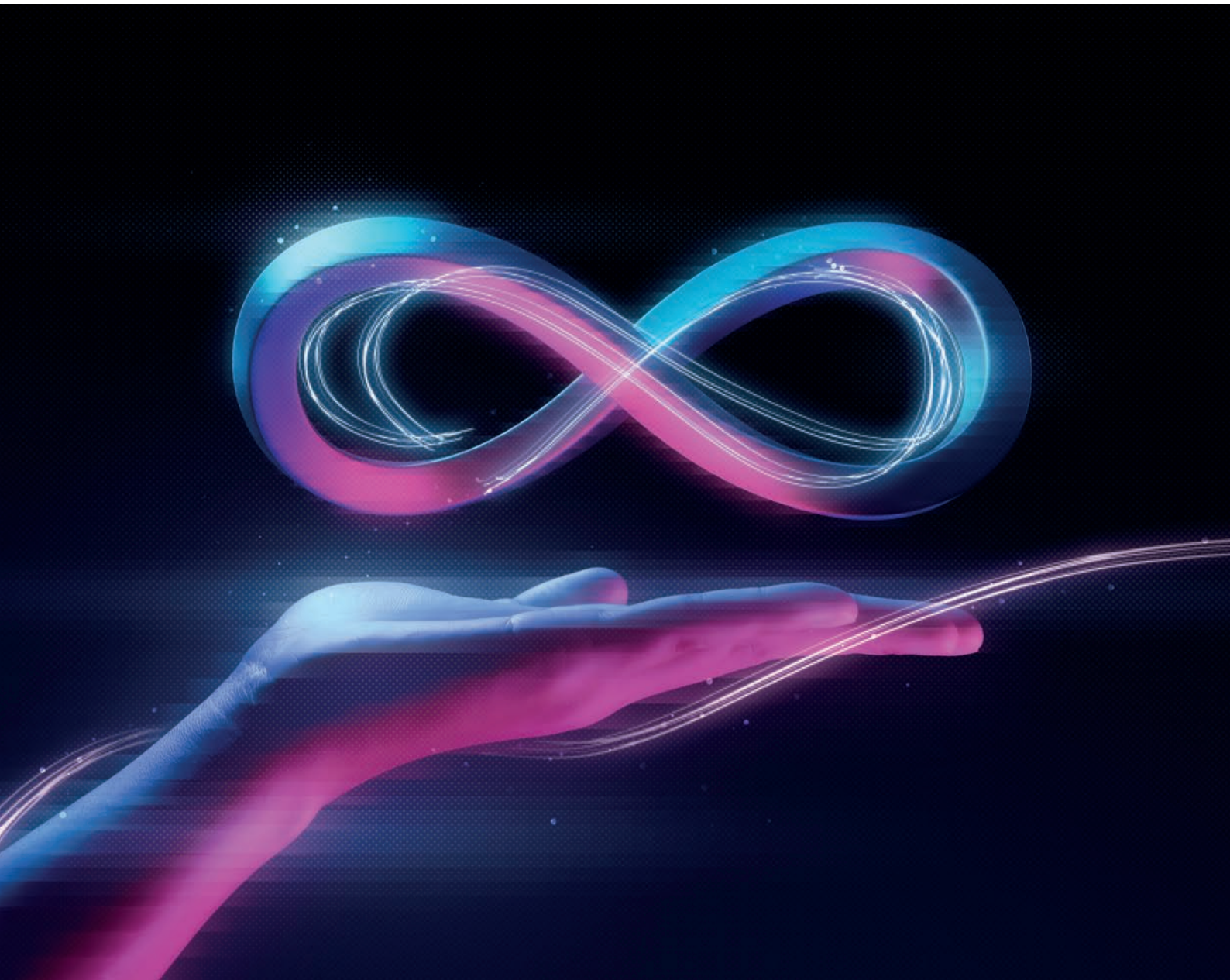
Jess Drabkin
Partner
New York
jdrabkin@reedsmith.com

Thomas Fischl
Partner
Munich
tfischl@reedsmith.com

Data protection and privacy

Today's privacy and data protection laws were built for physical filing cabinets and then updated for the internet. Applying them to tomorrow's metaverse, an alternate digital real-time existence offering a persistent, live, synchronous, and interoperable experience, could well prove to be a stretch too far.

The following sections describe some of the ways in which current privacy and data protection laws could potentially be applied to, or end up becoming obsolete in, the metaverse.



The datasets collected in the metaverse may be more numerous and extensive than ever

The technology, interactions, experiences, and interconnectivity of the metaverse could mean the collection of personal data on a scale we have never seen before. Although, inevitably, the actual data needed and collected will depend on the specific use cases that emerge.

While an avatar may likely be in a different form to its creator, the data collected in relation to and generated by it remains linked to the individual behind it and constitutes personal data. Such data may comprise information collected via familiar registration and payments to service interactions and systems data generated through log ins. However, what concerns many commentators, is the collection of new, even richer combined datasets in the metaverse including anything from gait, gaze, posture, emotion and haptic data involving sensations as well as interactions with other individuals, content and objects in real time. There is a potential that some such data may even constitute special category or sensitive data demanding higher protection under data protection laws.

The data sharing required for the metaverse to operate could be unprecedented

The sheer number of companies (not to mention legal entities) involved in making the metaverse tick could be on a scale never seen before. The intended experience for the user will require rich personalization, dependent on their profile, preferences, and actions.

Users will be able to move around between different metaverses so that multiple data sets can be collected or shared between different spaces of the metaverse.

Such mass personal data use brings various privacy challenges. A key problem is how to manage the sharing of such personal data and set up the contractual accountability and privacy obligations required to protect its use.

A further layered challenge sits in the fact that additional contractual requirements apply in many countries where personal data is transferred out of certain jurisdictions. Transfers out of the EU have been a particular focus area in the last year and now require careful assessment on a per transfer, per country basis. How will the metaverse take into account (or not) such requirements, given its all-encompassing, global reach and the aim to achieve freedom of movement within the metaverse? Will regulators be able to provide templates and guidance to allow the right balance between efficiency, pragmatism, and protection of privacy rights for individuals?

Furthermore, how can one determine any jurisdiction within the metaverse? This could ultimately be either the location of the user, the location of the avatar or the location of the relevant server.

The question of applicable privacy laws in the metaverse

The metaverse will connect the person to their “avatar” (or other digital representation(s)). Therefore, regulators around the world would likely consider information collected about a metaverse user’s activities to be personal data, subject to existing privacy and data protection laws.

As those who have practiced privacy and data protection law know, the cross-section of applicable laws, especially in the United States, is a constant challenge. Regulation of a digital interaction may involve the engagement of privacy rules in some countries based on physical location of the organization or the individual; the type of organization or individual (say, a health care organization or a child); the type of data collected (say, race or sexual orientation); and the purpose for collecting the data (for example, marketing or profiling). Applying this cross-section of laws is unwieldy even in a relatively static environment like the internet. It is unclear how organizations could navigate legal compliance in a persistent, live, synchronous, interoperable digital

environment. Organizations operating within the "one-stop-shop" privacy rules of the EU General Data Protection Regulation (GDPR) may fare better here, but this raises another issue – which privacy rules of which country apply in the metaverse? Does it still make sense to have privacy laws such as the California Consumer Privacy Act (CCPA), which focuses on Californian residents, and won't the metaverse make it even harder for organizations outside of the UK and Europe to know when they are targeting products or services to or monitoring those in the UK and Europe and therefore caught by the GDPR?

Further, who will be held responsible for privacy in the metaverse? We don't know what (if anything) will own or control some or all of it. Possibly, it will operate with single-organization ecosystems (similar to today's social media platforms), centrally operated platforms hosting different organizations offering their goods and services, but alternatively, it will be characterized by interacting access points and multiple controllers. If governments hold organizations responsible for others' activities in the metaverse, it is difficult to envision organizations building anything but a collection of proverbial "walled gardens" that will not fulfill the promise of the metaverse.

Determining who is responsible will be challenging

In a metaverse, diverse entities will be present and a web of relationships and encounters will emerge, making it difficult to determine who is responsible or liable within these different relationships. With regard to applicable data protection laws, it will also be particularly challenging to determine who can be considered a controller and who a processor in the context of processing personal data.

Some commentators about the metaverse state that one of its key features is that "no one controls the metaverse" (although others have different views and it is certainly the case that many walled garden private metaverses exist today). Ultimately, however, if no one is supposed to control the metaverse, can there be any data protection responsibility at all?

Even in a virtual life, relationships and encounters, both private and business-related, must be protected and regulated by a legal framework, especially in order to protect fundamental rights. Following on from the question of the applicable legal regime in the metaverse, the GDPR, for example, could be applied under certain circumstances. Under the GDPR, the data controller would then be the entity that alone or jointly with others decides on the purposes and means of the processing of personal data (Art. 4 No. 7 GDPR).

The definition of the extent of decision-making possibilities regarding the purposes and means of the processing of personal data in the metaverse for individual entities seems particularly problematic in this context. On the one hand, it is conceivable that responsibility may be determined for a respective space within the metaverse, similar to the case with platforms or individual companies. Responsibility could also be seen to sit with access point providers, i.e., individual service providers that enable users to access the metaverse, such as internet service providers. This could lead to almost intolerable provider liability for individual service providers.

Or is the metaverse a starting point to move controllership and responsibility to the data subjects – who carry their data in their wallets and give participants in the metaverse access? Such a vision of the metaverse would not sit well with the current framework for data protection control and responsibility that has been designed for digital platforms and services today and could demand a full rethink.

Operationalizing transparency and control in the metaverse could stretch notice and consent models to their limit

A central theme of most privacy laws around the world require the use of notice and consent, which has led to lengthy privacy policies and multiple just-in-time notices. The last few years have seen an acceleration in such requirements with an ever-growing list of details that organizations need to tell their customers. For example, in the United States, if a company is using data for cross-context behavioral/targeted advertising, it must notify users and provide them with an opt-out under the

requirements of five new privacy laws coming into effect in 2023. These laws have a variety of new requirements involving notice and choice. For example, these laws will require a business to provide notice and consent if data is going to be used for a new purpose that is unrelated to the initial purpose of collection. This means that as services grow and evolve, so do the corresponding notices. Users are now confronted with pages and pages of privacy notices and pop-up consent banners. This model was developed for desktops and large displays and is already proving difficult for mobile users. The metaverse proves an even greater challenge, as the layers of data use by multiple parties will mean lengthy privacy policies, as well as layers of pop-up notices.

Detailed notice and consent at each interaction will not be operational in the metaverse. Imagine your journey through the metaverse being interrupted with notices about the various entities that collect and use your data. Then consider that each interaction in the metaverse will present you with endless controllers that will tailor their content (i.e., your metaverse) based on the user (i.e., the user's personal data) and what they have permitted. For example, one user may not have opted in to a new secondary purpose for her data use – does that mean that her journey will stop? These are the challenges that companies in the metaverse face as they juggle the development of new interactive frontiers with brands and entertainment developers, while also keeping an eye on the various privacy regulations around the globe.

This is not an entirely new journey for some businesses. Companies collecting data from residents of the EU and UK have already been grappling with the requirements for cookie pop-up notices, which are the bane of many. Now, as a result of the new laws, will users be confronted with pop-ups and clickwraps at every turn? At what point does visibility, consent, and choice over data use become unworkable and no longer in the interests of those it serves to protect? Or, will we need another solution, one that is made for this new frontier? This would be the hope of many who are developing content and interacting in the metaverse.

Determining which individual rights apply, who is responsible for complying, and how to operationalize them will be a difficult undertaking

Many privacy laws around the world give individuals rights with regard to their personal data, and individuals are increasingly aware of those rights. As a result of these mounting laws, individuals are now even more conscious of their ability to "access" or "delete" their information. In Europe, users refer to the right to delete as the "right to be forgotten," which proves to be a challenge for some businesses, depending on the length of time the consumer has interacted with the company and the nature of their services. In addition, many organizations in the last few years have dealt with requests from consumers and even employees (or ex-employees) to "delete all of the data immediately!" or "provide all of the data that the company holds on me." As those who deal with such requests will know, it's not that simple in practice and, for every right, there exist additional exemptions and exceptions. However, all requests need to be carefully considered on a case-by-case basis, and companies need to take time to consider how to inform individuals about their rights and to comply with requests within the required period of time.

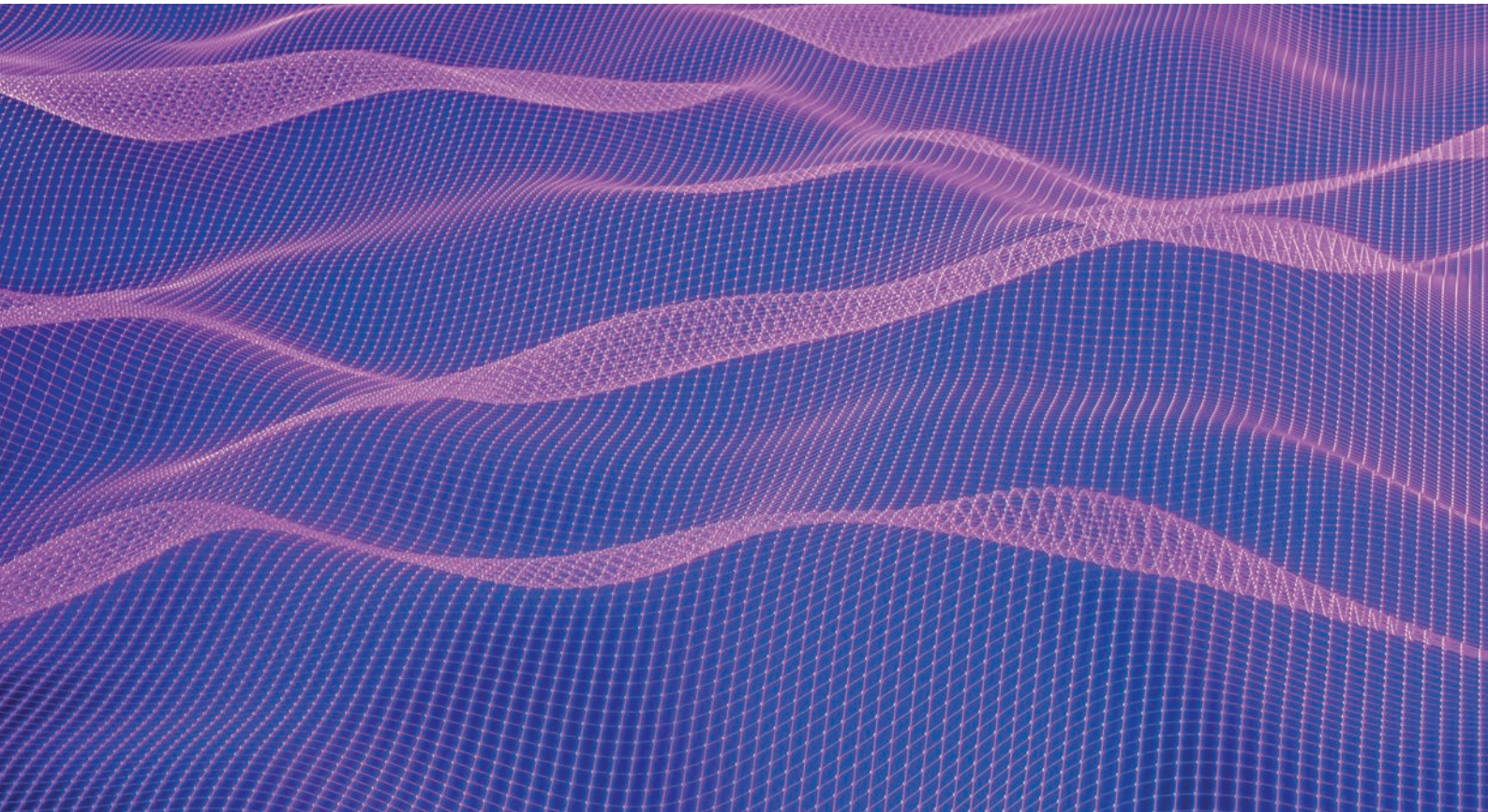
Applying this in the metaverse, the first issue to consider will be which rights apply to which individuals? As discussed above, the issue of jurisdiction is also applicable here. Today's privacy laws largely focus on the physical location of the consumer. In a physical world this makes sense. But in a digital universe that is borderless, not so much. It would seem the laws should attach based upon the physical location (or residence) of the user as a first step but the analysis would not end there. We'd have to consider all the laws that could attach to the user as she travels through the metaverse and engages with different services and content, which are offered by companies in multiple jurisdictions. She may have the "right to correct" as a result of her interactions with a European business, but she may not have the same right for a company operating from Japan. This leads to complicated questions of what rights does the user legally have as a result of her physical location, and

what rights does she have as a result of her interaction within the metaverse? Then, operationally, how will the functionality to exercise these rights be built into the metaverse? Again, pop-ups and lengthy notices are not an ideal solution.

AdTech and the metaverse

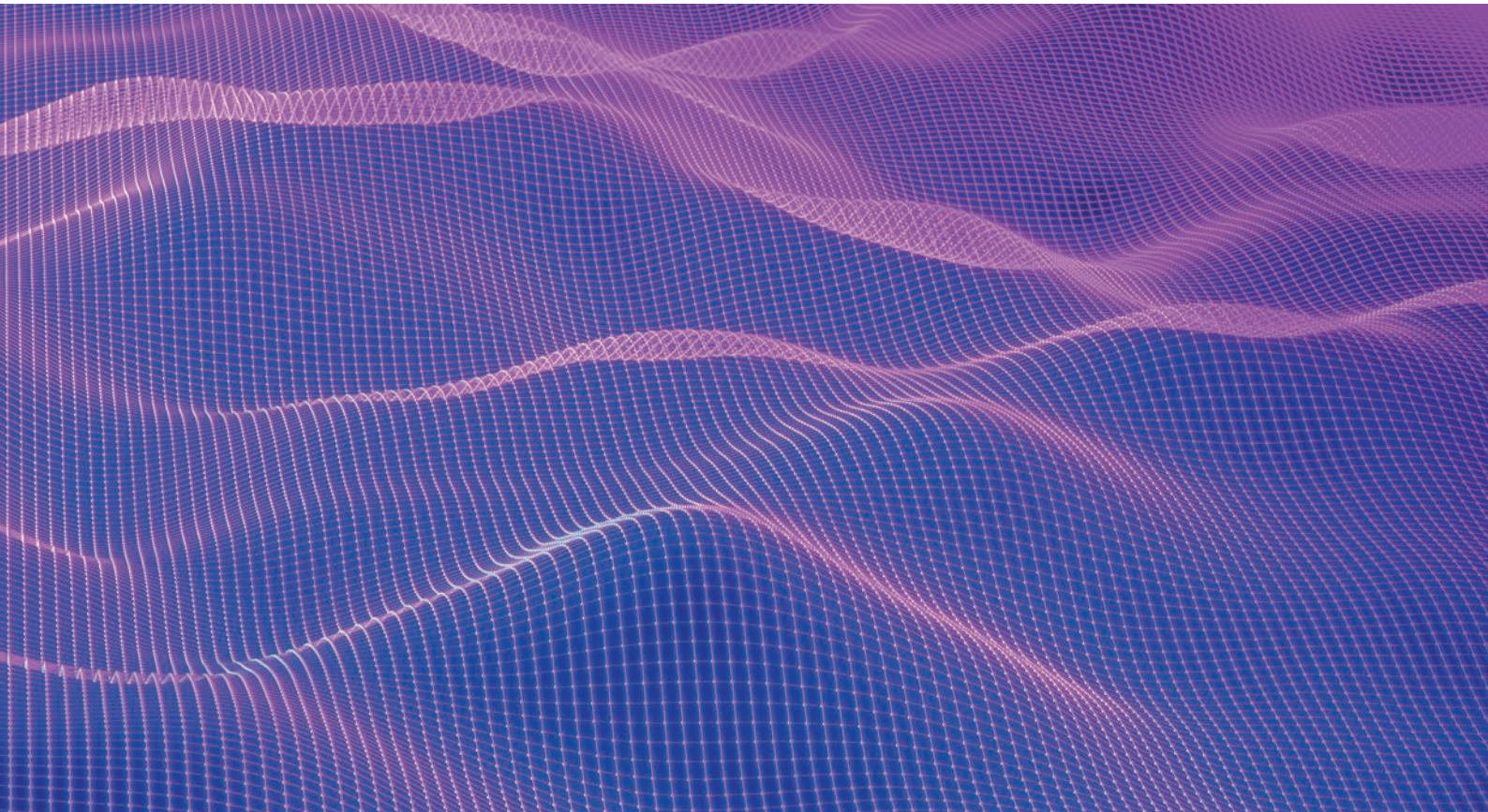
AdTech already exists in the gaming industry where providers give advertisers opportunities to place advertisements in-game, such as on billboards or jerseys and other in-game items, and the AdTech ecosystem has begun to find a way to support advertising opportunities in the metaverse. Besides the obvious data and privacy issues addressed above, typical issues that advertisers consider when contracting with an AdTech provider are obligations around compliance with laws, representations and warranties, indemnities, insurance, and ownership and licensing of data. However, there are other issues and concepts that are relevant in today's advertising landscape that will likely also be relevant to advertising opportunities in the metaverse:

- Measurement and cross-platform tracking of ads for attribution purposes is already an issue in the advertising industry generally, especially in light of the imminent demise of third party cookies and the ever-changing landscape of privacy laws. Advertisers should ask: How does measurement and tracking of ad performance in the metaverse work? Will acronyms like CPM and CTR no longer be relevant? How are standards set? Who is responsible for measuring ad performance? How will this technically be achieved? Will technology, such as eye tracking, be deployed to provide more accurate reporting?
- Ad fraud is any activity that fraudulently represents online advertisement impressions, clicks, conversions, or data events in order to generate revenue. There is no doubt that fraud will be present in the metaverse as well. Advertisers should ask: How can we prevent, track and measure fraud in the metaverse? How can we understand whether it is different to the fraud the advertising industry already grapples with?



- Viewability is the advertising metric that aims to track only impressions that can actually be seen by users. This metric will likely be relevant to at least some advertising opportunities in the metaverse. As such, advertisers should ask: How will we know if the ad is viewable? Are viewability standards different in the metaverse – or should they be?
- Brand safety is a set of measures taken to protect the image and reputation of a brand from the negative or damaging influence of questionable or inappropriate content when advertising online. Advertisers should consider brand safety issues when engaging in the metaverse and ask: How can AdTech providers help to ensure that advertisements are placed in brand-safe environments? What do I know about the metaverse I'm going to participate in and what are the community standards?
- Given that the metaverse, like the internet, will not be centrally owned, this brings about questions on how technically ads will be displayed. Advertisers should consider how contractual liability for this will flow through to the appropriate parties, from publishers to tech stack providers.

These are just some of the many considerations that arise when trying to apply existing data protection laws in the metaverse. It will be fascinating to see what changes will need to be made in practice either to the metaverse to suit existing privacy laws, or to existing privacy laws to suit the metaverse.



Children's privacy in the metaverse

The past few years have seen a marked soar in the protection of children's data protection rights, with the advent of the UK Age Appropriate Design Code, the German Interstate Treaty for the Protection of Minors in the Media (Jugendmedienschutz-Staatsvertrag), and the Irish Fundamentals for a child-oriented approach to data processing to name just a few initiatives. Again, the issue of the convergence of rules for different jurisdictions raises its head when we think about the metaverse, here with there even being fundamental differences as to when an individual is a child and when they become an adult, let alone the detail. The potential for mass data collection and targeting presented by the metaverse, discussed earlier in this chapter, run contrary to any of these developments in kids privacy however, begging the question as to whether we will see robust age gating to bar children from metaverse experiences, or the development of parallel kids-friendly metaverses.

Authors

Elle Todd
Partner
London
etodd@reedsmith.com

Joana Becker
Associate
Munich
jbecker@reedsmith.com

Tom Gates
Associate
London
tgates@reedsmith.com

Hubert Zanczak
Associate
Chicago
hzanczak@reedsmith.com

Keri Bruce
Partner
New York
kbruce@reedsmith.com

Charmain Aw
Counsel
Singapore
caw@reedsmith.com

Andreas Splittgerber
Partner
Munich
asplittgerber@reedsmith.com

Wendell Bartnick
Partner
Houston
wbartnick@reedsmith.com

Sarah Bruno
Partner
San Francisco
sbruno@reedsmith.com

Content exploitation

The metaverse will continue to provide new opportunities for content creation, consumption, and exploitation. However, the successful monetization of such content presents new challenges for stakeholders. In short, rights holders who create and license content will want robust protection to ensure that they are fairly remunerated for each new form of exploitation. In contrast, licensees who acquire and exploit content will want licenses sufficiently broad to adapt to the evolving use cases. End users' interests will be primarily focused on the user experience, but their interests may also overlap with those of rights holders and licensees, subject to whether they participate in content creation or consumption. Regardless, it is clear that the metaverse is changing the way we think about content licensing.

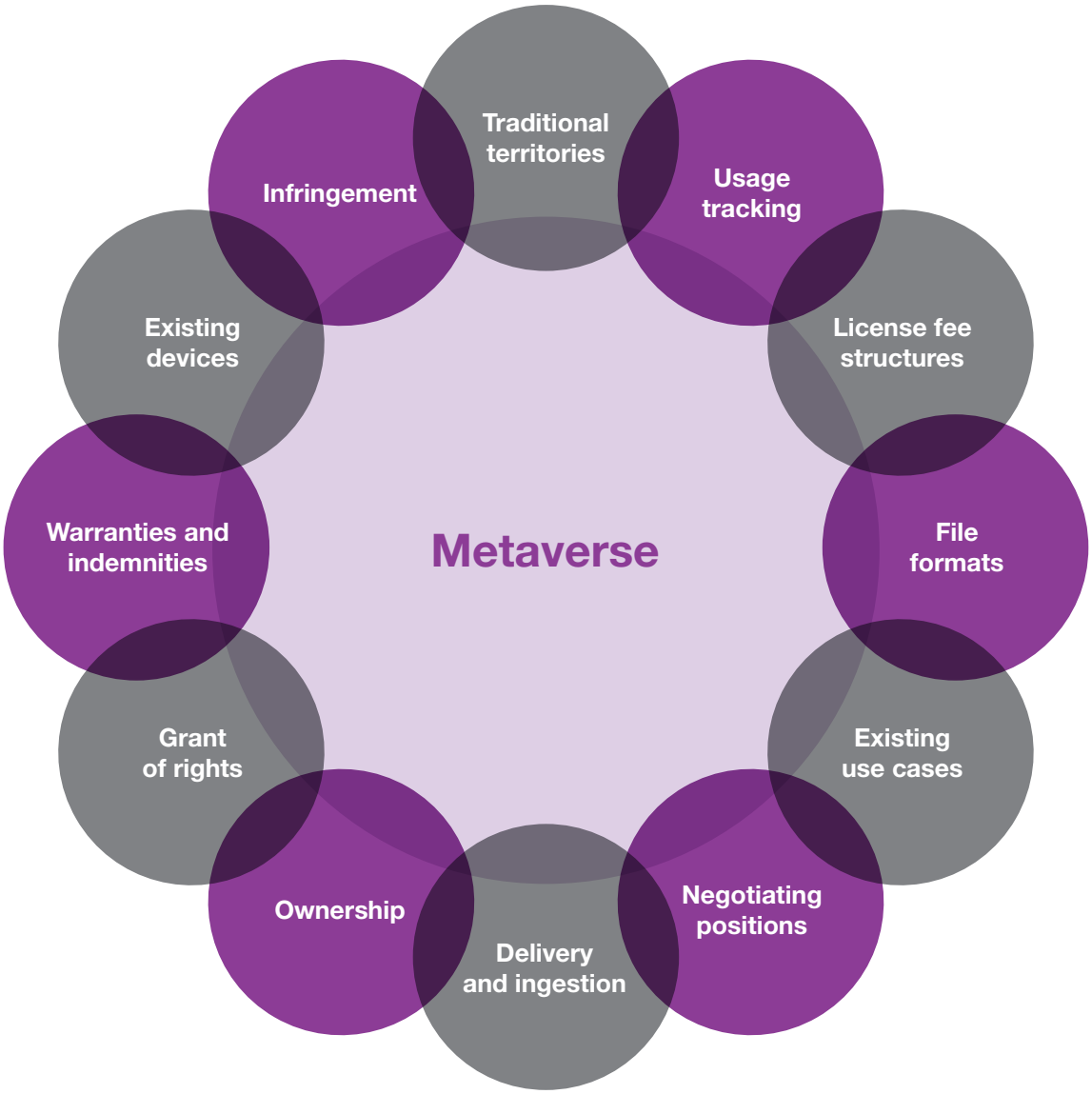
Key challenges

While the terms of any license will vary depending on the content and use case, among other factors, there are several common factors that will need to be carefully considered when licensing content for use in the metaverse, as further set out below.

Term	Current position	Implications for licensing parties
Territory	Licenses are typically granted on a territorial basis, with the licensed territory being defined at a national, regional, or worldwide level. Some agreements specify "the universe" as the applicable territory.	Is the metaverse included in existing territorial definitions? When air travel became popular, the rights to in-air entertainment were carved out so that they could be licensed separately. This may also be the case with the metaverse. As the metaverse continues to grow, we will continue to see the creation of new virtual worlds. To exploit content in these environments, licensees and licensors will need to consider how the virtual world is defined. This is particularly relevant in the context of augmented reality where real and virtual worlds may overlap. Licensees also may seek to include provisions granting them a right of first refusal for new virtual worlds.
Ownership	There are well-established laws and principles governing ownership of copyright in audio, audio-visual, and other traditional content formats. Any person intending to exploit third-party content is required to identify and then obtain a license from the copyright owner.	The metaverse will create new opportunities for AI-generated content. However, as in the real world, there are challenges in establishing ownership of such content, which means there will be additional challenges for anyone seeking to further exploit content that has been created by AI. As the metaverse extends beyond traditional territorial boundaries, licensors will need to ensure they can evidence adequate territorial ownership. This will require particular diligence where the licensor is an intermediary who had obtained its rights from the original content creator.

Term	Current position	Implications for licensing parties
Rights granted	The owner of a piece of content has certain exclusive rights in that content by way of copyright and other intellectual property rights laws. A licensor will grant certain rights to use the content, depending on the licensee's intended use case.	While basic copyright principles, as further set out in the *Intellectual property* section, will likely translate into the metaverse, the use cases are likely to be incredibly broad and constantly evolving. From a licensee's perspective, a grant of rights will need to be broad enough to adapt to the constantly changing environment without the need to repeatedly amend and renegotiate the underlying license. For example, the law remains unsettled on what rights are required to exploit content through NFTs, so it is important for licensees to obtain as broad a grant of rights as possible. Licensors should also review any exclusive grants of rights they have made to determine whether there is scope to argue that the metaverse falls outside the exclusivity conditions. To the extent the content contains any underlying third-party rights, whether intellectual property or publicity rights, the licensor will need to ensure that it can pass those rights on to the licensee. In addition, to the extent that a piece of content (for example, a clip from a music video, television show, movie, video game, or commercial) was produced under one of the many SAG-AFTRA collective bargaining agreements, the creator of such content must ensure the licensee's compliance with any payments due to the performers as a result of the licensee's use of the content.
Negotiating positions	Traditionally, the bargaining power between licensors and licensees has been determined by several key factors, such as (i) who the more powerful entity is, (ii) whether the licensor has a monopoly on the rights being granted, (iii) the perceived value of the content, and (iv) whether the licensee is under pressure to obtain a license (for example, if it was previously operating without a license). Often, this results in major licensors having a strong bargaining position in content licensing negotiations.	The metaverse will likely continue to disrupt the power balance between licensors and licensees by presenting new opportunities for content exploitation and enabling less established licensors to make their content available. There will also likely be more opportunities for individual or independent content creators to distribute their content directly, which may mean greater competition for original content. This could result in licensees being required to offer more attractive licensing packages to obtain licenses for original content.
Licensed services, devices, and uses	Licenses are often limited to a particular service, device, or use (or a combination thereof). For example, a licensor may grant a license that allows end users to stream music through a branded service on named devices.	The interactivity of the metaverse may make it more challenging for licensors and licensees to agree to limit the license to specific use cases. Licensees will likely demand greater flexibility to facilitate the development of and interaction with the metaverse, while licensors will want to rein in the grant of rights as tightly as possible and maximize the number of licenses that can be granted in connection with the same content. As licensors and licensees become more attuned to how content is exploited in the metaverse, key use cases will likely develop as industry standards for granting rights, subject to the further evolution of the metaverse.
Fees	A license fee may be based on a flat fee, a fee per subscriber, a fee per viewer hour, minimum guarantees, advances, proportions of revenue, or other usage models (or a combination thereof) in exchange for the grant of rights from the rights holder.	While the basic fee mechanisms may remain the same, the metaverse will complicate (1) the definitions of revenue and usage metrics; (2) how usage can be tracked across different services, devices, and use cases; and (3) how the fee is calculated. Fees may also be impacted by the collective bargaining obligations referred to above. Additionally, the metaverse tends to attract alternative payment structures as parties may agree to cryptocurrencies or digital wallets. Licensors and licensees alike will need to make sure they are well versed in the laws governing both, and what implications they may have on their businesses.

The above is by no means an exhaustive list of the challenges the metaverse brings to content licensing, but it represents some of the key commercial and legal issues that will need to be considered by licensees and licensors. Flowing from these overarching considerations are other challenges that will also need to be assessed, such as usage tracking, file format standardization, delivery and ingestion of content, scope of warranties and indemnities, and conduct of claims for infringing use, among others.



Different perspectives

Inevitably, licensors and licensees will have different perspectives on these key challenges. Licensors will likely seek to maintain a restrictive approach to licensing in the metaverse, for example, by limiting the grant of rights and clearly defining the licensed services, devices, and uses, unless there is a substantial financial incentive otherwise. The underlying considerations will remain the same – licensors want to control how their content (and ultimately their brand) is used and consumed. Licensees typically want as broad a license as possible, as this allows them to be more creative with content exploitation and to take advantage of market developments and trends. This will be even more important in the metaverse, as the rights implicated in certain key use cases, such as the exploitation of NFTs, remain subject to debate. Service providers with existing licenses will need to determine whether such licenses are sufficient. The reach, immediacy, and interactivity of the metaverse will demand the broadest set of rights possible, and it will likely be more important than before for licensees to negotiate rights of first refusal for new forms of exploitation or new digital worlds. Licensors and licensees will need to consider the overarching user experience when negotiating the scope of the grant of rights. The licenses that facilitate content exchange in the metaverse will need to be flexible enough to ensure a seamless user experience between increasingly overlapping and interconnected services. This may force conservative licensors to provide greater flexibility regarding bundling and associated limitations, but equally makes it ever more important for licensors to ensure that their reputations and brands are adequately protected (as further set out in the *Deepfakes in the metaverse* section).

“This may force conservative licensors to provide greater flexibility with regard to bundling and associated limitations, but equally makes it ever more important for licensors to ensure that their reputations and brands are adequately protected.”

Key industries

While there are some key challenges that will apply across a variety of different sectors (as further set out in the *Advertising*, *Games*, and *Music* sections), different industries will face their own particular issues in terms of content licensing in the metaverse.

Advertising – The right to include a song or other item of content in any form of advertising is often strictly controlled. Even if such rights are granted, they are often subject to numerous restrictions and approvals, such as payment obligations to performers, singers, and musicians under the various SAG-AFTRA and American Federation of Musicians (AFofM) collective bargaining agreements. While the licensee may not be a signatory, the licensor will typically include a specific provision that requires the licensee to nonetheless comply with such collective bargaining agreements. In addition, rights holders want to ensure that their content is not being used to promote a product they do not support, or in a way that does not fit with the creator's image. This will be even harder to manage in the metaverse because there will be numerous scenarios in which a particular advertisement is viewed, depending on how the viewer interacts with the metaverse. In the United States, individuals appearing in the content being licensed (including deceased individuals) may have rights of publicity that require permission for the use of their likenesses (including digital ones) in advertising. The metaverse will likely become a source of advertising inventory (for example, virtual billboards, point of sale at virtual stores, event sponsorships, etc.), raising questions regarding how best to track and measure the effectiveness of and engagement with virtual advertisements. Similarly, there will be sponsorship and branding opportunities, and sponsors will need to consider the extent to which any real-world restrictions on these activities will apply in the metaverse.

Games – Gaming and eSport companies will most easily be able to adapt their existing services and operations to function seamlessly in the metaverse. Because of this head start, "players" in this industry should, on the one hand, carefully consider how to protect their content and assets while also exploring how they can license out their rights to other less metaverse-ready industries. On the other hand, the traditional use of buyout models in the content creation process means they are not constrained by a limited grant of rights. Companies operating in this space will likely be the leaders in pushing the boundaries of content licensing as the metaverse continues to grow.

Music – Usage tracking poses a particular challenge for music licensing in the metaverse, particularly when you layer in the SAG-AFTRA and AFofM payment requirements for songs recorded under their collective bargaining agreements (which includes most songs from major labels). With different services, devices, and use cases, the likelihood of receiving duplicate or triplicate claims for a single use are even greater. Already complex and expensive usage tracking and reporting systems will need to be adapted to deal with the interactivity inherent within the metaverse. Existing collective management licensing structures will also need to be examined, particularly considering what rights such entities will hold in the metaverse and whether they will continue to license on a territorial basis.

Social media – The terms and conditions for the use of social media services set out intellectual property ownership provisions, but the increased interactivity across services and devices in the metaverse will likely blur the lines between where one service begins and another ends and, therefore, which terms will be controlling and also who owns the IP created. Similarly, if a user creates a piece of content in one corner of the metaverse, questions will arise as to how it will be licensed in another area and who will be liable for any infringing use. Increasingly, end users may demand compensation for any such exploitation – meaning that service providers will need to consider how revenues can be shared across different services and devices.

Film and TV – We are already starting to see increased interactivity in how we view film and TV – take, for example, interactive TV and films on Netflix, such as Bandersnatch and You vs. Wild. As the metaverse continues to grow, there will likely be additional opportunities to exploit existing audio-visual content formats within the metaverse as well (think of movie theatres and branded digital merchandise for your avatars). There is more opportunity for increased interactivity between content creators and viewers in the metaverse, both with and between viewers and also with their surroundings, which will create new opportunities for content origination and funding, and may also impact how stories are told. This may also raise ownership issues: to what extent does the viewer transition to a creator who holds certain rights in the content, and what does that mean for continued exploitation of the content? Also, what does it mean if the interactivity leads to infringement of another party's rights? And who is liable: the producer or the interactive viewer?

What you can do to prepare

As the metaverse evolves, we will see an influx of the development of new services and devices to facilitate user engagements. New entrants will need to prepare bespoke agreements for how content is licensed. At the same time, existing service and device providers will transition their services to fit the metaverse, and they may wish to review existing content licenses to determine whether they are sufficient. For the reasons set out above, this will not be an entirely straightforward exercise as there are new challenges to consider in the metaverse. Existing stakeholders will need to either enter new licenses or amend existing ones to build in the flexibility necessary to operate successfully in the metaverse.

Authors

Jess Parry
Associate
London
jparry@reedsmith.com

Hannah Kong
Associate
London
hkong@reedsmith.com

NFTs: Ownership in the metaverse – the birth of a new concept

Ownership, a legal concept almost as old as humanity, is being tested by the advent of the metaverse. The staggering rise in popularity of non-fungible tokens (NFTs) demonstrates how much appetite there is for a solution capable of replicating the personal ownership enjoyed in the real world.

The advent of the metaverse, an always-online, persistent, spatial "second" world, represents a fundamental shift in our notion of digital frameworks and presence, but metaverses – literally, beyond the universe – are not entirely new concepts. Videogames like the 17-year-old game Second Life and more recent games such as Fortnite, Roblox or The Sandbox – a platform where users can buy virtual land and create, play and monetize their creations on the blockchain – may all be labelled early versions of immersive metaverses.

At its core, a metaverse is code: ones and zeros, overlaid with unfathomably vast amounts of data; a manufactured environment in which all assets are synthetic, created and experienced from within. In such a world, everything comes from code. From the clothes our avatars wear to the car we drive in, our "things" can only exist in the metaverse after being coded.

From a legal standpoint, our immersion in this entirely digital world poses a challenge to a number of legal concepts that have arisen out of the material world, including the fundamental concept of "ownership." Important questions, such as whether virtual assets qualify for "ownership," or whether new forms of ownership will emerge from the metaverse, are going to demand attention from users of the metaverse, and potentially from lawmakers, as the world transitions into virtual environments.

Property and proprietary metaverse(s)

Ownership (or "property") is a legal concept that is almost as old as humanity. Prehistorians believe that it is the emergence, during the Neolithic period, of a sedentary life and agriculture that gave birth to the concept of property, a basis upon which our capitalistic societies continue to be run today.

Property rights of all sorts – in real estate, in shares of a corporation and in musical compositions, to take three examples – give their beneficiaries a monopoly over a resource. The recognition of this monopoly is generally seen as stemming from the idea that it gives the owner an incentive to invest in improving the property because it receives benefits from its use or sale. Accordingly, a "proprietor" or "owner" can exercise exclusive possession or control over an object.

Intellectual property (IP), in particular copyright, has been created to enable a similar reservation of rights for its beneficiaries. The companies building the metaverse are no stranger to this; as many other entertainment businesses, the architects of the metaverse use IP rights to protect and monetize their investment. In fact, there is a clear incentive for these businesses to build proprietary virtual worlds, where all that is created – software, graphic elements, characters and features – qualifies for IP protection.

This new world, in which "IP is everywhere," will present challenges and interesting legal issues for the users of the metaverse, whose expectations, forged in a world of brick and mortars, may not always transpose in the metaverse. After all, if I can own a car in real life, what stops me from owning the same in the metaverse?

Ownership vs. licensing: A well-documented tension

Since the internet was invented, a number of landmark cases have illustrated how users of certain digital "goods" want the goods to replicate exactly the same tangible goods in the real world.

In *Usedsoft*, a case heard by the Court of Justice of the European Union (CJEU) in 2011, the debate regarding the legal capacity for software purchasers to resell their "used" software licenses on a secondhand market captured the attention of the entire digital world; could software licenses be resold or, rather, "novated"? In 2018, in *Capitol Records v. Redigi*, the U.S. Court of Appeal for the Second Circuit was asked the very same question in relation to users who wanted to sell their legally acquired digital music files, and buy "used" digital music from others at a fraction of the price currently available on iTunes. More recently, a Dutch company by the name of Tom Kabinet also took its case all the way up to the CJEU, to try and obtain a recognition that e-books could be legally resold, secondhand.

The outcome of these cases is well known: Software, digital films, digital music and digital books cannot be resold on a secondhand market, for they are not "owned" by their purchasers in the first place, but licensed.

With tangible items, there are two separate forms of property that can be exercised: There is the property of the tangible item itself, in the form of the paper, the disc, the plastic box, etc., while separately, there is also the intellectual property (i.e., copyright) in the book, music, software or film. By contrast to tangible property, IP can only be appropriated by the persons designated by the law as benefiting from the copyright (generally their authors). When a work loses its material element, such as when a book or a compact disc becomes nothing more than a file, there is no equivalent digital "property" in the file that can be acquired separately from the intellectual property. A digital file ultimately only comprises data in the form of zeros and ones, and data – or information – cannot be "appropriated" in the same way a physical object can be. Information and data, just like ideas, are free-flowing.

The three cases mentioned above illustrate the continuous tension existing between the expectations of users of digital items and the companies that are licensing them. In *Usedsoft*, the only decision where the CJEU did not entirely rule out the possibility of transferring secondhand software licenses, the dominant narrative was that it would be "unfair" not to allow the existence of a secondhand market, and an undue restriction of consumers' rights, which probably explains why the court went to such length to try and find an acceptable middle ground.

Today, the narrative that consumers may be unduly restrained keeps resurfacing and, while owners of IP rights have so far managed to successfully contain the idea that digital goods should be tradable, it will become increasingly difficult to convince the users of the metaverse that their assets merely exist by way of a limited metaverse end-user license agreement. As in the real world, users are far more likely to claim the right to "own" the virtual handbag, land or car they just "bought" in the metaverse.

Why not simply make it clear that metaverse items are in fact licensed? The solution is tempting but seems unrealistic. For users of digital items, limited licenses are often seen as an imperfect substitute for "ownership." This is further illustrated by several socioeconomic theories that have demonstrated our human attachment to ownership as a concept, including that of the "endowment effect." According to this theory, individuals place a higher value on an object that they already own than the value they would place on that same object if they did not own it (for example, if they merely received some limited controls over it). This theory, which seems widely accepted, could explain why digital items are so rarely advertised as being licensed, and so often presented as being "sold" to customers. In brief: Ownership sells, licensing does not, yet there is nothing to be "sold" in a virtual world, and that is the gigantic paradox that the metaverse users and builders will need to confront.

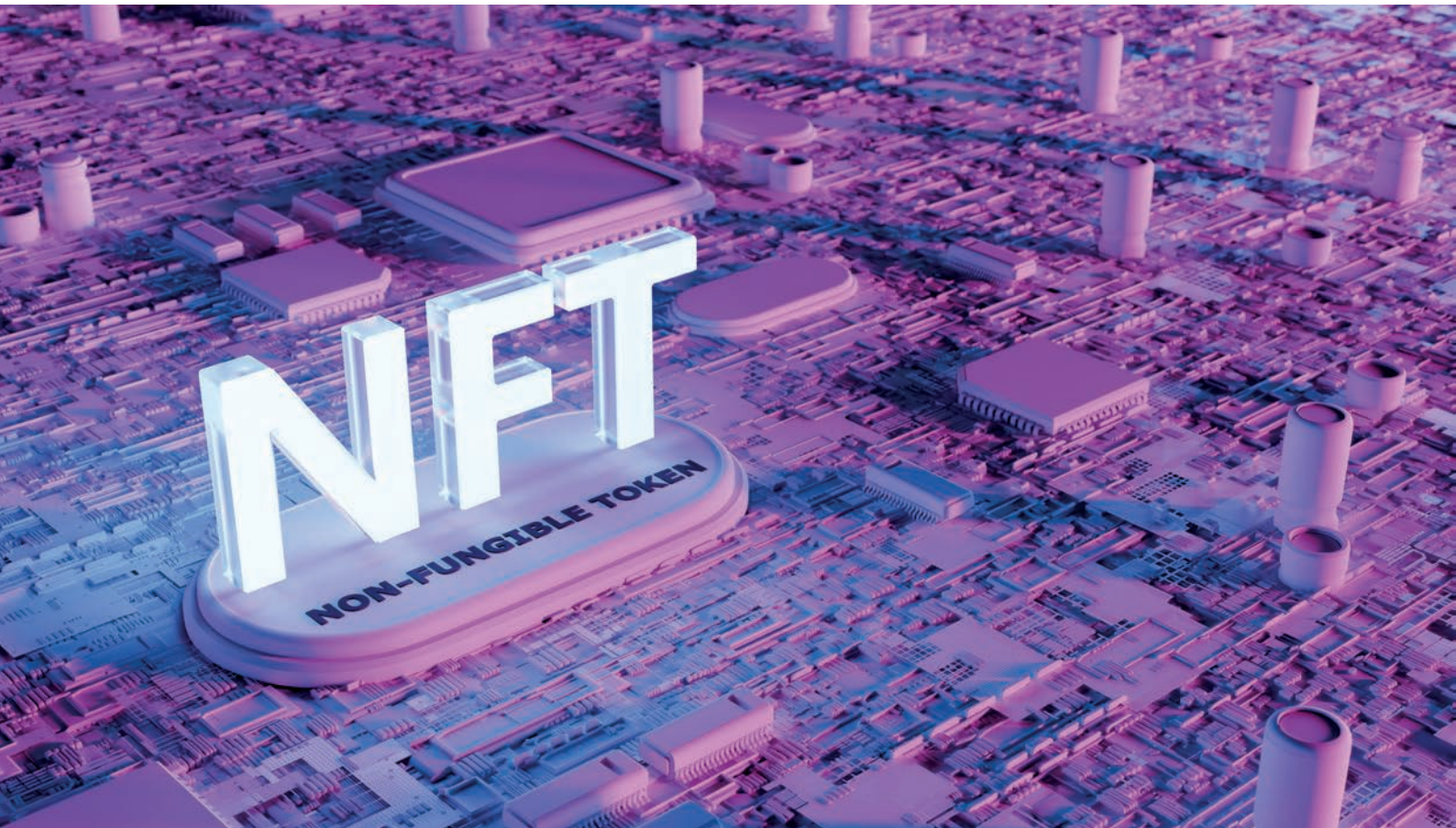
Enter the NFT

The staggering rise in popularity of NFTs demonstrates, if anything, how much appetite there is for a solution capable of replicating the personal ownership enjoyed in the real world.

From a legal standpoint, the concept of NFTs is ingenious and yet very simple: If one cannot own a digital item made of free-flowing information, then let's find something else that may be "owned," separately from the intellectual property. For example, an unfalsifiable certificate of authenticity associated with that digital item. Authenticity certificates, issued by the item's creator in very small numbers, are indeed a very clever way of recreating scarcity and a sense of ownership and therefore of value, without the need to assign or transfer IP rights to the acquirer of the token. What is being traded here is a unique connection with the digital work and, most importantly, the much sought-after feeling of ownership, be it only of a token encapsulating a certificate.

This is where the NFT magic operates, where the millennium concept of property is once more reinvented, by being displaced from a tangible medium (disc, book, tape, etc.) to an intangible certificate. To think, notarial certificates of authenticity were already proposed by Usedsoft as a way to enable the reselling of software licences back in 2007 – a solution both remarkable and logical, and a promise of what was to come.

Today, the proponents of the secondhand market for digital goods are not alone in rejoicing: The whole industry is suddenly reinvigorated by the concept. Christie's and Sotheby's, two pillars of auctioneering, are enthusiastically selling NFTs of works that never before entered the sanctuary of these respectable houses for they could not be "felt" or made unique. From Beeple's "Everydays: the First 5000 Days" to drawings Andy Warhol made digitally, creations once banned from the auction market are being tokenized and making a remarkable entrance on the art market.



Digital ownership reinvented?

If NFTs appear to be solving a lot of the problems that arose when trying to grant impossible ownership rights over digital items, including by embodying a clever resale right mechanism allowing the initial offeror of the NFT to participate in the profit generated by each resale, a bigger question is whether NFTs will fulfill our ownership expectations. An NFT does not confer a monopoly over a work, nor does it permit its holder to decide how the work will be used, distributed or shown. By the once-enjoyed monopoly of an art collector being displaced from that exercised over the object itself to that exercised over a certificate, it is our entire understanding of the concept of ownership that may be changing. What this shift is saying about our human values is both fascinating and ominous. Welcome to the "meta-propriety."

Crypto-assets, in practice

In version 1 of this *Guide to the Metaverse*, we explained that respected legal commentators have suggested that some common law systems (English law in particular) may well have sufficient flexibility to expand the application of property law to certain types of purely informational crypto-assets. Since then, there have been two court decisions, in the UK and Singapore, that have established that NFTs may be capable of being property in their own right. In the UK, in an interim judgment,[10] the English High Court found that there was an arguable case that NFTs are property under English law, giving owners important proprietary remedies to enforce their rights over third parties. In practice, this means it is arguable that, distinct from the item it represents, the NFT token itself is capable of being owned. These developments are certainly positive for web3 advocates who see NFTs as the key to unlocking true ownership over digital assets.

Importantly, this property right is in respect of the token itself, rather than the off-chain asset to which the token relates. This nuanced distinction is critical and often not appreciated by the average NFT purchaser, leading to potential confusion over what purchasers are "buying." In the case of artwork NFTs, while the token itself is freely transferrable and tradable as a distinct form of property, the NFT owner's right to use the associated underlying artwork will be governed by established intellectual property principles.

Intellectual property: What IP rights are granted to NFT holders?

No two NFT projects are the same and what rights are granted to purchasers vary widely. We typically see three broad types of IP treatment for NFT projects:

- No IP rights granted. A significant proportion of NFT projects we have reviewed make no reference to IP rights and grant no express permissions to use the underlying IP. From a legal perspective, purchasers in these instances are purchasing a service from the seller in the form of an authentication of a work of art.

  The value of the NFT comes from the verified provenance it guarantees through the blockchain (i.e., that the NFT can always be traced back to having been issued by the artist).

- IP license granted. Some NFT projects often grant purchasers express license rights to use the underlying works in particular ways. Often these licenses are carefully drafted and provide limited rights for the NFT holder to display the work associated with their NFT for personal purposes. However, inspired by the iconic "Bored Ape Yacht Club," there are a rising number of creators taking a different approach to intellectual property and starting to give NFT holders commercial usage rights over their NFTs.

  "Bored Ape Yacht Club," one of the most successful NFT projects to launch in 2021, gives holders an "unlimited, worldwide license to use, copy, and display the purchased Art for the purpose of creating derivative works based upon the Art." Some holders have taken full advantage of this, with Adidas sporting a Bored Ape as its official web3 avatar and itself launching a derivative NFT; Universal Music's 10:22PM label signing a new group called Kingship, consisting of four characters from "Bored Ape Yacht Club;" and one ape being signed with CAA for future commercial opportunities.

- IP rights assigned. In rare circumstances, we have also seen NFT projects seek to transfer legal ownership of IP through NFTs. When the NFT is traded on the secondary market, the seller assigns all of their IP rights in the underlying work associated with the NFT to the purchaser.

  Giving away IP rights to NFT holders is a credible idea in principle, but it does inadvertently trigger various legal issues. The vast majority of people buying NFTs are not used to conducting due diligence on their purchases, and the marketplaces for NFTs are simply not set up to accommodate this. Conducting chain-of-title analysis of digital assets that are traded like stocks is near impossible.

The key takeaway from this is that purchasers of NFTs should understand what they are "buying." Equally important is for those tokenizing artwork to be careful in how they market and advertise their NFTs. Advertising the "sale" of artwork could be potentially misleading if all the NFT creator is offering is a digital certificate. As we learn from behavioral economics and the endowment effect, the temptation might be strong to advertise NFTs as nothing less than a "sale," but the consequences of doing so might be fraught with serious legal issues.

The (smart) contract issue

A key feature of NFTs is that they are (or ought to be) liquid and thus easily tradable. This is what gives them their apparent value and why we are seeing digital assets being sold and bought for millions. But where the NFT is nothing more than a license, how liquid can the license really be? A typical license agreement invariably offers some form of warranty or indemnity from the licensor to the licensee, against anything disturbing the quiet enjoyment of the rights granted, but if the NFT changes hands 20 times, who will stand behind the content?

Another challenge of using NFTs to "sell" certain limited licenses or usage rights over digital artwork is knowing how to effectively "attach" the contract or terms and conditions to the NFT such that the purchaser (and future purchasers) of the NFT is bound by them. A related question is, how can a seller or marketplace easily enforce the terms of those contracts against the applicable purchaser? Sellers and marketplaces have to walk a fine line between ensuring they impose appropriate terms on purchasers of NFTs and ensuring those NFTs can be traded easily and with little formality. The more sophisticated the usage rights are, the more critical it will be to ensure that the seller imposes robust contractual restrictions and remedies on purchasers. Sellers will need to bear this in mind when choosing the marketplace through which to sell NFTs.

The hosting issue

We have established already that NFTs comprise information that relates to another asset. More often than not, the asset to which an NFT relates is stored "off-chain." Due to capacity issues, it is too expensive and resource-intensive to host content on a blockchain. Typically, only basic pixelated artwork is hosted on the blockchain itself (such as CryptoPunks, an NFT collection of 10,000 profile pictures). Hosting the asset on the blockchain itself is recognized as being as close to full decentralization as possible; the asset will be available permanently for so long as the supporting blockchain continues to operate.

The majority of NFT projects host the associated assets on third party servers. The smart contract to each NFT (or at least each Ethereum ERC-721 standard NFT) contains a universal resource identifier (URI) that provides for the online location of the associated NFT asset. The URI operates like a traditional hyperlink to a location from which the NFT smart contract pulls the relevant asset.

Certain projects (particularly those launched by web3 native brands) choose to use decentralized or distributed forms of hosting for their NFT assets (such as IPFS or Arweave) that operate on a peer-to-peer basis. While this is currently the best alternative to on-chain storage for a decentralized solution to storage, it does raise a number of issues, particularly for rightsholders. Once content is uploaded to IPFS, it is almost impossible for it to be removed, leading to potentially significant consequences in cases where the asset infringes third party IP.

The alternative that many brands choose to implement for their NFT projects is good, old-fashioned, centralized storage. Naturally this gives brands the best form of control over their assets, but if a brand can simply take down or change the NFT work, this does arguably undermine the decentralized promises of web3 and democratization of digital content. Indeed, this is precisely what web3 is trying to prevent. Nevertheless, to what extent the masses will expect, demand or care about this level of decentralization remains to be seen.

Regulation, regulation

There is no specific regulation yet regarding NFTs, but the carefree attitude of early adopters should not serve to elude the reality: NFTs are regulated exactly like any other type of asset you can buy online. As transaction volume grows, we suspect there will be greater scrutiny applied by regulators, authorities and watchdogs. While the issues will be as numerous as there are NFTs, three compliance issues deserve a special mention.

1. **Securities regulation**. As described above, NFTs have been designed to carry a number of similar characteristics to a financial asset. Although they are not fungible, NFTs have been encouraging, and used as a tool for, speculation. Consequently, it is possible that they may come to be regulated within financial regulation, but the question is still open. One of the primary factors that will determine whether an NFT is a security is the purpose for which it is being created and sold. If the NFT is being created and sold as a way for members of the public to earn investment returns, then that type of NFT is more likely to be considered a security. Those considering minting an NFT should take advice before doing so to avoid unintentionally breaching financial regulatory law. Even the way in which the NFT is described and marketed can influence the extent to which it may be considered falling within the scope of securities law, and we foresee some marketplaces and sellers coming unstuck if they do not consider this seriously.
2. **Consumer law**. NFTs are offered to the public; they are not restricted to professional buyers only. Accordingly, marketplaces and sellers are subject to local consumer law, which requires them to operate with a high level of transparency and brings them within the scope of consumer protection laws on unfair commercial practices, including the right for consumers to withdraw, to receive appropriate information about the NFT in their local language, to subject the NFT sale to their local law, etc.
3. **Tax law**. The nature of the transaction will determine its tax status (is it a sale or a license, a national or an international transaction, B2C or B2B, etc.?). The tax treatment will also be different for marketplaces, sellers and purchasers. With the high fluctuation in prices, it will be critical to obtain proper tax advice to understand your exposure to sales and other taxes.

In conclusion, NFTs may be fun experiences, giving people special access to something they personally value (like an unreleased track by your favorite band, or a digitally signed artwork), but those looking to make a solid investment should understand the risks and limitations attached to NFTs and not let the sirens of digital ownership replace a robust due diligence exercise.

Authors

Sohie Goossens
Partner
London
sgoossens@reedsmith.com

Nick Breen
Partner
London
nbreen@reedsmith.com

Is my NFT a security?

As NFTs continue to surge in popularity, questions swirl around their legal and regulatory status. For some NFTs there is lingering uncertainty on issues such as the ownership rights they convey to the buyer, whether the NFT can qualify as "property" under applicable legal frameworks, and which consumer-protection principles should apply to the sale and purchase of the NFT.

With NFTs being structured in an increasingly complex manner, an additional question that now commonly arises is whether the NFT qualifies as a regulated financial product under the laws governing its issuance and distribution. In their purest form, NFTs represent unique items such as collectibles or pieces of art that are not intended to be a financial product, notwithstanding that they may represent an attractive investment opportunity (as is the case of many non-financial real-world items). But when NFTs give their holder the right to income streams or to a share in an underlying portfolio of investment assets, the NFT potentially transforms into a regulated financial product. With the increasingly exotic structuring of rights attaching to NFTs, the conventional industry perception that NFTs are unregulated products is gradually eroding.

Use cases for NFTs with complex tokenomics abound. Such NFTs are, for example, integrated into play-to-earn gaming platforms, where they may represent avatars or other in-game items that can be used to generate income for the holder. NFTs may also be minted as an on-chain representation of a unique real-world asset that a decentralized autonomous organization (DAO) wishes to invest in, thus giving the DAO participants collective exposure to the value of that asset. A further noteworthy development is the emergence of platforms that issue NFTs that give their holders rights to a share of royalties generated by underlying music catalogues. In some cases, payments made to holders of the NFT may be automated via smart contract, for example where the NFT is issued on the Ethereum blockchain using the ERC-721 or ERC-1155 standard, both of which have proven popular in the NFT space.

Financial regulatory frameworks around the world generally function in a technology-neutral manner – i.e., they apply to digital tokens that have features of financial products irrespective of how the token is labelled or presented, and regardless of whether the token is offered or supported by a company that does not otherwise operate in the financial sector. Accordingly, a token – whether fungible or non-fungible – that gives the holder ownership or control rights in a business or portfolio of assets, or which entitles the holder to certain income or revenue streams, may qualify as a regulated product such as a security or a unit in a collective investment scheme. In determining which regulatory frameworks to consider, the relevant jurisdictions are usually those where the NFT is issued and those where users are located.

Determining whether an NFT is a regulated product is important because the issuance, offering, marketing and distribution of such a product will typically give rise to a raft of requirements that apply in the financial services sector, and non-compliance with these is usually an offence. These may include, for example, a requirement for the issuer and distributors of the NFT to be licensed or approved by the relevant regulator(s) and to comply with ongoing conduct-of-business requirements (e.g., in relation to disclosure of information to purchasers of the NFT, fitness and properness of personnel involved in running the NFT offering, etc.). Establishing and maintaining frameworks to ensure compliance with these requirements typically requires a high degree of

specialism and significant human and financial resource. While an NFT offering may be run within the confines of exemptions and may thus avoid regulation, typically such exemptions will only allow the offering to be directed at sophisticated investors in the wholesale markets and will not enable any offering to the retail public.

Consequently, issuers and distributors of NFTs whose core operations are situated in sectors such as entertainment and media or gaming will typically not wish to upscale and retool to meet the onerous requirements of financial services regulation, and will instead collaborate with appropriately regulated industry partners or will seek to structure their offering in a manner that avoids the NFT becoming a regulated product to begin with. Factors that potentially help mitigate the risk of an NFT qualifying as a security or other regulated product include the following:

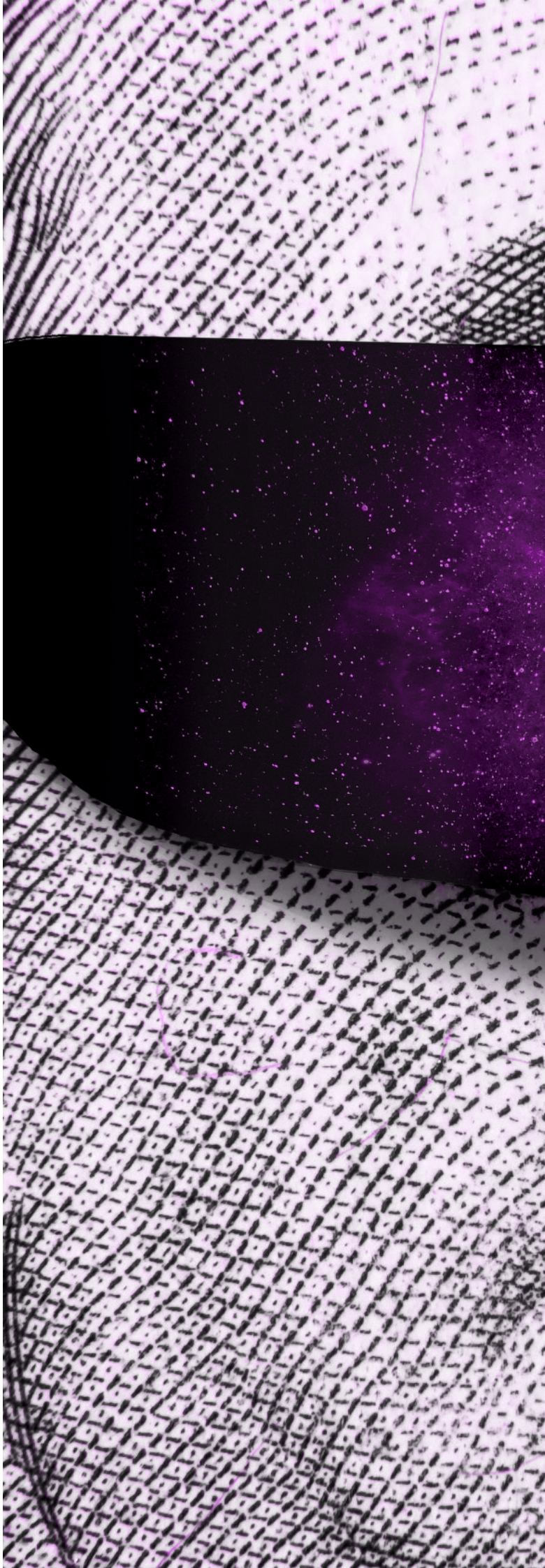
- Tokenomics: In some cases it may be possible to avoid an NFT qualifying as a security or other regulated product if returns accruing to the NFT holder need to be earned by the holder on the NFT's native platform, rather than the holder having a passive entitlement to such returns. In this case it may be possible to characterise payments received by the NFT holder as being part of a simple commercial quid pro quo because they represent consideration for the holder performing actions that are useful to the NFT's native platform (such as staking or exercising platform governance rights).
- Decentralization: If the NFT is issued by a DAO or other protocol that is fully decentralized (i.e., it is governed solely by the community of protocol participants, without centralized control being exercised by any particular person), it may be possible to argue that the NFT, even if it has features of a security, does not qualify as a security because decentralization prevents the relevant product definition from applying. For example, where an NFT has features of a debt note (i.e., periodic fixed-interest payments are made to the holder) but is issued entirely on-chain and is not booked as a debt liability on the balance sheet of any entity, it may be possible to argue that the NFT does not qualify as a debt security. However, legal arguments of this nature that rely on decentralization remain largely untested with the regulators and courts, and they may not be future-proof given that regulators are increasingly focused on how to approach the supervision of decentralized finance.
- Offshoring: Where the NFT does constitute a security or other regulated product, an option that some NFT issuers consider is to establish their issuer company in an offshore jurisdiction and launch a website for their platform that is generic and not directed at users in any particular location. The platform then refrains from conducting active marketing in any location and relies solely on users on-boarding themselves to the platform on a reverse-solicitation basis. However, this approach may not be aligned with what most NFT platforms wish to achieve, because it precludes any marketing. It is also not risk-free because some jurisdictions in which users are based may not recognize reverse solicitation as a means of avoiding regulation. Furthermore, it would always be advisable to use geo-fencing to exclude users in some high-risk jurisdictions (e.g., the United States), even if they approach the platform at their own initiative.

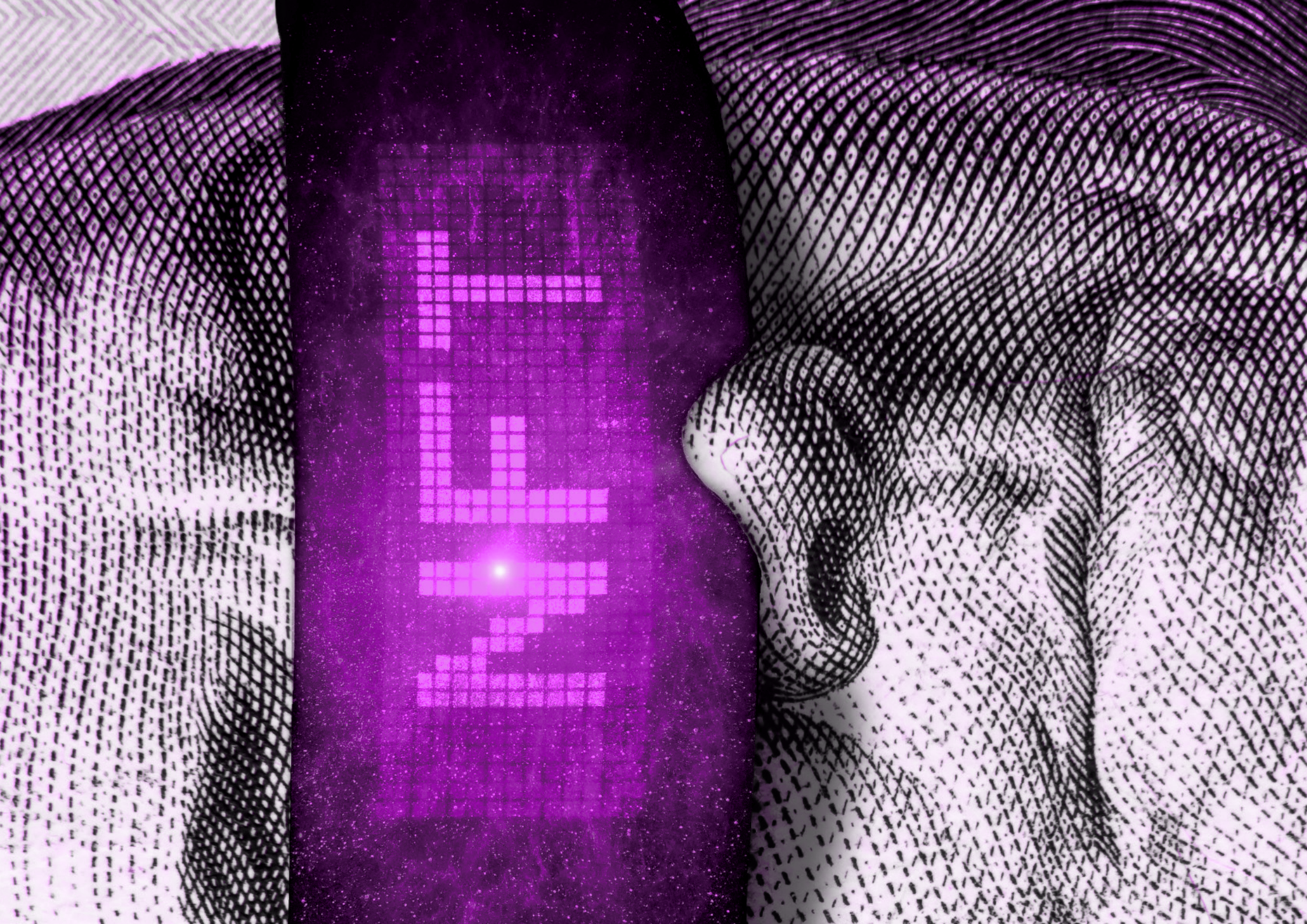
As the structuring options for NFTs multiply, developers, platforms and other stakeholders involved in the NFT issuance and distribution process need to remain alive to the financial regulatory implications. Navigating the relevant frameworks and confirming the regulatory position should be treated as a key part of the product development process, as the consequences of inadvertent non-compliance can be costly. Appropriate structuring is key to ensuring that the product remains on the right side of the regulatory perimeter.

Authors

Hagen Rooke
Partner
Singapore
hrooke@reedsmith.com

Nina Carlina Sugianto
Associate
Singapore
ncarlina@reedsmith.com





The ultimate NFT?

Fraudulent paper bills of lading have long plagued the trading, financial and logistic industries. The system of bills of lading dates back at least a few hundred years and has largely been unchanged. However incidences of fraud have continued unabated and a trio of cases in Singapore involving counterfeit and duplicated bills of lading racked up billions of dollars of losses for banks and counterparties in 2020. One possible solution to this problem is by digitization. Following work done by the United Nations Commission on International Trade Law (UNCITRAL) and promoted by the International Chamber of Commerce (ICC), a solution in the form of the UNCITRAL Model Law on Electronic Transferable Records (MLETR) has arisen.

MLETR aims to enable the use of electronic transferable records (ETRs) both domestically and across borders, by recognizing the legal validity of ETRs that are functionally equivalent to their paper-based counterparts. MLETR recognizes the additional requirements which documents transferring ownership and title in goods require and relies on the additional safeguards afforded by distributed ledger technology, thus introducing electronic bills of lading (eBLs). MLETR has been ratified by countries such as Bahrain and Singapore. The G7 and the European Union have also begun steps to implement MLETR in their member countries. Commercial parties such as Maersk, COSCO, HSBC, DBS, Fonterra, Syngenta and Transfigura are all piloting or implementing eBLs.

One favoured protocol to implement eBLs is the ERC-721 protocol, which is also used for a number of NFTs. The eBL is the digitization an already existing commonly used commercial document representing billions of dollars or more of trade annually and solves a longstanding and ever-increasing fraud problem. This is possibly the ultimate NFT.

In the same vein, countries are digitizing their trading systems by setting up single windows that they interface and interoperate with other single windows of other countries in their region to form regional single windows such as the EU Single Window and the ASEAN Single Window where verified parties such as approved traders may submit trade documents digitally to government and other parties. The principles of this structure of walled gardens interconnected and interoperable with other walled garden bears an uncanny resemblance to a metaverse.

Author

Bryan Tan
Partner
Singapore
bryan.tan@reedsmith.com

Investing in crypto

There are over 19,000 different cryptocurrencies, including stablecoins, that have been generated and made available for sale and trading on various exchanges. Bearing in mind the various warnings that governments, such as those in the UK, Israel, the United States, and Singapore, have issued regarding investment in digital assets – including specific warnings about scams and the advertising restrictions on crypto advertisements to the general public that have been enacted in the UK, Spain, and Singapore.

We have set out some basic due diligence steps when investing in cryptocurrencies. Of course, where necessary, professional advice should be sought.

- Mode of investment: Most purchases of cryptocurrencies will be from exchanges. Then, upon payment, the cryptocurrencies will be sent to a hot wallet, typically hosted by the exchange. In some cases, the cryptocurrencies are obtained directly from the token generation event in a process called the initial coin offering. However, there is a class of cryptocurrency transactions that use cold or unhosted wallets where the technical assistance and transaction mechanism of an exchange will not be available. In this case, extra care should be taken, as discussed below.
- Research: Conduct thorough research on the cryptocurrency. Read and understand its business model and tokenomics, and check out the background of the key team. The website, the white paper, and the accompanying contractual documentation should set out clearly and consistently the entities involved with the cryptocurrency.
- Whether the cryptocurrency is listed: Although not conclusive, a listed cryptocurrency indicates that there is a ready market should you need to liquidate. If the exchange is reputable, it will also have done some level of basic due diligence.
- Security measures: Cybersecurity hacking incidents such as those relating to Solana, Harmony, and Axie Infinity have given rise to the term cryptojacking. A significant investment requires that some due diligence be carried out on the cybersecurity measures employed by the token issuer or platform as crypto companies have been targeted by hackers.
- Anti-money laundering/know your client (AML/KYC): Transactions involving regulated wallets will already have AML and KYC features built in. For transactions involving unhosted wallets, AML and KYC measures will be necessary – especially for significant transactions. In the EU, the proposed transaction floor for required reporting is €1,000. In all transactions, the source of funds must be determined in order to ensure that the cryptos being transferred are not the proceeds of criminal activity.

A final note on significant unhosted wallet crypto transactions – in order to ensure that the transaction is executed smoothly and with reasonable levels of privacy for the parties, practice has evolved to includes measures and techniques such as zero knowledge proof (where information is exchanged to validate the transaction with high probability without revealing confidential data such as wallet addresses), proof of coin (the crypto equivalent of proof of funds), and the Satoshi test (to demonstrate control over a specific address).

Author

Bryan Tan
Partner
Singapore
bryan.tan@reedsmith.com

Crypto and other digital assets: Europe, the United States and the United Arab Emirates

We have reviewed the relevant regulatory and commercial environment in Europe, the United States and the UAE.

Crypto and other digital assets: Europe

In September 2020, the European Commission published a draft regulation on crypto-assets, the so-called Markets in Crypto-assets (MiCAs) regulation. The European Parliament adopted its negotiating position on March 14, 2022, which cleared the way for the formal "trilogue" between the European Commission (the Commission), Council, and Parliament. On June 30, 2022, the trilogue negotiations resulted in an agreement whereby, after formal adoption by the Council and the Parliament, the regulation could enter into force over the course of this year. Then, according to the current draft, it would take effect 18 months after its promulgation.

As a regulation, MiCA will have direct effect in all EU member states, while creating an EU-wide and uniform set of regulations with regard to crypto and other digital assets. It contains measures to achieve objectives such as transparency, disclosure, authorization, and supervision of transactions in relation to the distribution, issuance, and trading of crypto and digital assets. This is intended to create comprehensive consumer protection and at the same time establish measures against criminal activities such as market manipulation, money laundering, and terrorist financing in all EU member states.

MiCA imposes strict rules regarding the authorization and licensing of financial intermediaries and therefore will have the greatest impact on issuers, service providers, and trading venues – which, however, serves the interest of achieving a secure EU-wide crypto financial market.

Measures such as increased information requirements with the aim of informing potential buyers about the characteristics, function, and risks of crypto token and digital assets are enshrined in detail. The requirements for the information document to be prepared for this purpose – the so-called "white paper" that must be submitted to the relevant financial supervisory authority – are regulated in article 5 of the MiCA regulation.

It must include detailed descriptions of the issuer, the issuer's project, and the type of crypto-asset to be offered or for which admission to trading is sought. Also required is a description of the rights and obligations associated with the crypto-assets and the disclosure of information about the underlying technologies and standards that the crypto-assets issuer uses to enable holding, storing, and transferring the crypto-assets. Likewise, a detailed description of the risks associated with the respective assets is mandatory.

MiCA also includes rules on capital requirements for custody of assets and a mandatory complaint procedure available to investors. Issuers of significant asset-backed cryptocurrencies (global stablecoins) would be subject to more stringent requirements, for example, with respect to required capital, investor rights, and oversight.

Further, MiCA determines that crypto service providers, such as crypto-asset custodians and operators of trading venues, must have a registered office in a member state if they want to offer their products and services in the European Union.

For smaller companies and fintechs, these provisions could cause certain disadvantages. In member states where the market has been virtually unregulated to date, companies face high costs due to, for example, the acquisition of licenses or the costs incurred in connection with reporting requirements or a secure IT infrastructure. It is therefore foreseeable that the regulation will make it more difficult for cryptocurrency issuers to enter the market.

However, once licensed, the strict rules allow for fewer legal and administrative hurdles when intermediaries enter another EU market in another member state with the goal of expanding their financial services. The reason for this is that once a crypto intermediate is licensed in one EU member state, that license can become "passportable" under MiCA, meaning that the intermediate could choose to operate in another EU country without having to obtain further approval or additional licenses from the local government. The current patchy legal framework in different European countries makes it difficult for companies to start a business in this still new area of the capital market. In addition, the different national regulations create unequal opportunities for market participants. Against this backdrop, the possibility of "passporting" could provide for simplification in the future.

A central innovation is the regulation of the future supervision of issuers and crypto-asset service providers by the European Supervisory Authorities and the national authorities. According to MiCA, the European Securities and Markets Authority is to supervise the issuance of asset-referenced tokens, whereas the European Banking Authority will be in charge of supervising electronic money tokens. To distinguish between the individual crypto-assets, the regulation provides a set of definitions of the different crypto-assets, including utility tokens and certain types of stablecoins and thereby undertakes a categorization of different crypto-asset types, each with different legal consequences.

In terms of sustainability, it must be noted that the EU Parliament's and Council's proposal on MiCA envisaged a total ban on individual cryptocurrencies. This is not against the backdrop of regulatory difficulties, but is due to the negative impact on the environment caused by high-energy consumption in the process of mining the currency – so-called proof of work. Such a ban, however, has not prevailed.

For the crypto industry, it is relieving that a ban on proof of work was not adopted, as corresponding provisions would otherwise have limited the development of the crypto market in the EU.

Nevertheless, even if there is no ban, the EU continues to make efforts to stimulate environmentally friendly investments in order to reduce the high carbon footprint that is inevitably connected with some cryptocurrencies. Members of the EU Parliament have urged the Commission to prepare a legislative proposal by January 1, 2025, to include in the EU taxonomy a classification system for all crypto-assets that contribute significantly to climate change. Currencies that operate outside the proof of work mechanism and that subsequently have a lower carbon footprint could then be considered "green" according to the EU Taxonomy Regulation.

MiCAs' impact on German legal regulation regarding crypto and digital assets

When it comes to MiCAs' effect on the national German regulatory landscape, we anticipate that the new regulation will not have an extensive impact on existing national provisions since reporting obligations and the handling of crypto-assets specified in MiCA are already covered by existing financial regulations in Germany. For this reason, Germany is considered a good entry point for companies looking to enter the European crypto market.

This is because the existing national regulatory network is structured in such a way that it applies generally to financial instruments in Germany with which also relatively new crypto tokens that meet the relevant factual requirements are subject to the existing regulatory structure.

Applicable laws include the German Securities Trading Act, (Wertpapierhandelsgesetz), the German Securities Prospectus Act (Wertpapierprospektgesetz), the German Capital Investment Act (Vermögensanlagengesetz or VermAnlG), the German Investment Code (Kapitalanlagegesetzbuch), the German Banking Act (Kreditwesengesetz of KWG), the German Insurance Supervision Act (Versicherungsaufsichtsgesetz or VAG), and the German Payment Services Oversight Act (Zahlungsdiensteaufsichtsgesetz).

In the context of the question of whether a token is subject to the existing national regulatory framework, it should be noted that crypto and digital assets cannot be defined in a uniform manner. Without the examination of all individual circumstances and characteristics of the respective token, it is not possible to make a regulatory classification because of the diverse and different design of the numerous tokens that appear on the market.

One prerequisite for the regulations to apply would be that the token is a "financial instrument" within the meaning of section 1 (11), sentence 1 KWG. Although "crypto tokens" are not mentioned as a separate category in the KWG, in the sense of a technology-neutral interpretation, they may be included in the individual categories listed in section 1 (11), sentence 1 KWG, for example, in the category called "crypto-assets." It should be noted that, according to the German Federal Financial Supervisory Authority (BaFin), section 1 (11), sentence 1, No. 10 KWG is designed as a catch-all provision, as crypto securities may already fall under one of the other categories of financial instruments of section 1 (11), sentence 1 KWG because of their diverse design. This means that if the respective crypto token is already subject to one of the other categories in an individual case, a renewed license is not required.

This is advantageous for many banks, as they regularly already hold the necessary license to operate the custody business.

Whether the regulations apply is decided on a case-by-case basis and depends, again, on the legal structure of the token.

An NFT may fall under the definition of "crypto-assets" and then be regulated accordingly as a financial instrument under the existing regulatory framework, if it is created with the intention of generating monetary profits, and therefore the investment purpose is in the foreground when creating the NFT. This is also the case if the token holder ultimately acquires exclusively an asset position via the token ownership, but never takes possession of or uses the tokenized object itself. In such cases, it is also conceivable, for example, that the token may be classified as an "asset investment" under the VermAnlG.

Like NFTs, stablecoins can also be subject to the term "financial instruments" under German regulatory law. In particular, a classification as "units of account" or as "Crypto-assets" – according to the KWG or the German Securities Institutions Act – can be considered. This is because the legal definition also covers assets that are not alternative means of payment but serve investment purposes. Algorithmic tokens fulfill this purpose as a possible investment.

Also, crypto custody is covered by the existing regulations. The German Act Implementing the Amending Directive on the Fifth EU Anti-Money Laundering Directive (Gesetz zur Umsetzung der Änderungsrichtlinie zur fünften EU-Geldwäscherichtlinie) has introduced crypto custody business into the KWG as a new financial service. Pursuant to section 1 (1a), sentence 2, No. 6 of the KWG, crypto custody is defined as the custody, administration, and safeguarding of crypto-assets or private cryptographic keys used to hold, store, or dispose of crypto-assets on behalf of others, therefore qualifying as a so-called "financial service" under the KWG. In addition, crypto-assets themselves are also to be regarded as so-called "financial instruments" within the meaning of section 1 (11), sentence 1, No. 10 KWG, as crypto-assets are the digital representation of a value.

Therefore, with regard to the custody of crypto tokens, the custody is subject to authorization according to section 32 KWG. A corresponding license must be applied for at BaFin.

Just as the MiCA will demand in the future, financial service providers that wish to distribute banking and financial services products in Germany on a targeted basis must already have established a subsidiary (section 32 (1) in conjunction with section 33 (1), sentence 1, No. 6 KWG) or a branch (section 32 (1) in conjunction with section 53 KWG) in Germany in order to obtain the necessary license. In this respect, as well, the regulations in Germany are already in line with the new EU regulation.

Although Germany already provides a national regulatory network that covers crypto and digital assets, a common EU framework is welcome. Especially against the background of simplifying cross-border activities of financial service providers within the EU to achieve a stimulating effect on the crypto and digital assets sector, it is foreseeable that MiCA will bring real progress to the crypto financial industry market as a whole.

Authors

Simon Grieser
Partner
Frankfurt
sgrieser@reedsmith.com

Friedrich Lutter
Intern
Frankfurt
flutter@reedsmith.com

Crypto and other digital assets: United States

In the United States, the Securities and Exchange Commission and the Commodity Futures Trading Commission (CFTC) are the agencies that are most closely involved in the regulation of crypto and digital assets. The mission of the SEC is to protect investors; to maintain fair, orderly, and efficient markets; and to facilitate capital formation.

The SEC's approach to whether a digital asset is categorized as a security derives from application of the test set forth in the 1946 Supreme Court decision, *SEC v. W.J. Howey Co.* (referred to as the Howey Test). The Howey Test determined whether an asset constitutes an "investment contract," one of the enumerated types of instruments defined in the securities laws. The test states that an investment contract involves (i) an investment of money, (ii) in a common enterprise, (iii) in which the investor is led to expect profits, (iv) derived from the entrepreneurial or managerial efforts of one or more third parties.

The mission of the CFTC is to promote the integrity, resilience, and vibrancy of the U.S. derivatives markets. The CFTC seeks to protect the American public from fraudulent schemes and abusive practices in those markets. Under the Commodity Exchange Act (CEA); the CFTC has oversight over derivatives contracts, such as futures, options, and swaps, that involve a commodity. The CEA defines "commodity" to include agricultural products, "all other goods and articles," and "all services, rights, and interests...in which contracts for future delivery are presently or in the future dealt in."

While the SEC has suggested that many digital assets are securities, arguably, the two most important digital assets – bitcoin and ether – have been recognized as commodities by both the CFTC and the SEC.

In the United States, crypto and digital assets remain largely unregulated, with the crypto community often complaining that regulators have been regulating by enforcement. That appears to be rapidly changing in favor of more regulatory clarity.

On March 9, 2022, President Biden signed an executive order addressing the risks and benefits of digital assets – including whether the United States should establish its own Central Bank Digital Currency. "The rise in digital assets creates an opportunity to reinforce American leadership in the global financial system and at the technological frontier, but also has substantial implications for consumer protection, financial stability, national security, and climate risk," said the Biden administration in a White House press release. The administration stressed that "[t]he United States must maintain technological leadership in this rapidly growing space, supporting innovation while mitigating the risks for consumers, businesses, the broader financial system, and the climate. And, it must play a leading role in international engagement and global governance of digital assets consistent with democratic values and U.S. global competitiveness." The executive order represents the Biden administration's first step toward regulating the cryptocurrency market, which SEC Chair Gary Gensler has compared to the Wild West.

The executive order sets forth six key priorities for government oversight of cryptocurrencies: (1) consumer and investor protection; (2) financial stability; (3) mitigating illicit finance; (4) U.S. leadership in the global financial system and economic competitiveness; (5) financial inclusion; and (6) responsible innovation. While the executive order is a first step toward additional rules and regulations for digital assets, it does not provide any concrete guidance. The order, however, is likely to lead to additional regulation in the near future.

Since the executive order, regulators and legislators have begun to make their intentions clear.

On April, 4, 2022, SEC Chairman Gary Gensler provided remarks at a capital markets conference on the future of crypto and digital assets. Gensler compared crypto trading and lending platforms, whether centralized or decentralized, to traditional securities exchanges regulated by the SEC, and made clear that crypto platforms need to be registered and regulated to protect investors.

Gensler also discussed how stablecoins, a class of cryptocurrencies often backed by stable reserve assets, raise three important sets of policy issues. Gensler said that most crypto tokens are "investment contracts" (in other words, securities) under the Howey Test. Gensler emphasized the importance of getting crypto tokens registered with the SEC and requiring issuers of crypto tokens to comply with the SEC's disclosure requirements, noting that "[a]ny token that is a security must play by the same market integrity rulebook as other securities under our laws."

Gensler's comments on stablecoins are particularly interesting, because most critical observers of the United States' regulatory regime believe stablecoins to be within the purview of the CFTC, not the SEC. For example, in October 2021, the CFTC issued an order settling charges against the stablecoin Tether for making misleading statements in connection with the reserves for USDT, its stablecoin pegged to the price of the U.S. dollar.

Meanwhile, United States legislators seem to favor an approach that would bring much of the regulatory oversight for crypto and digital assets under the CFTC's umbrella. On June 7, 2022, U.S. Senators Kirsten Gillibrand, a Democrat, and Cynthia Lummis, a Republican, introduced the first major bipartisan crypto legislation. The bill would give the CFTC exclusive jurisdiction over digital assets, subject to certain exclusions. "Digital asset[s]" are defined as a natively electronic asset that confers economic, proprietary or access rights or powers, and that is recorded using cryptographically secured distributed ledger technology. It later defines virtual currency as a digital asset that is used "primarily" as a medium of exchange, unit of account, or a store of value not backed by an underlying financial asset.

Five types of digital assets are explicitly excluded from the CFTC's jurisdiction, and would be subject to the SEC's jurisdiction. The five types of digital assets subject to SEC jurisdiction include digital assets that grant the holder with any of the following rights with respect to a business: (1) a debt or equity interest; (2) liquidation rights; (3) interest or dividend payments; (4) a profit or revenue share derived solely from the entrepreneurial or managerial efforts of others; or (5) any other financial interest. In addition, the CFTC does not have jurisdiction over NFTs.

While the United States' regulatory regime remains in flux, it appears to be coming into focus quickly. Further, the Gillibrand-Lummis bill would appear to seek to make the United States attractive to crypto and digital assets by providing greater regulatory clarity.

Author

Mark Bini
Partner
New York
mbini@reedsmith.com

Crypto and other digital assets: UAE

The United Arab Emirates (UAE) has positioned itself at the forefront of virtual assets. In addition, according to reports, a comprehensive framework for all metaverse-related commerce and activity is in the works.

It is worth noting that the UAE is a federation of seven individual emirates, where each emirate is subject to individual rules and laws and all emirates are subject to federal law. In addition, there are several economic free zones in the UAE that have their own independent rules and legal frameworks. The most prominent free zones of the country are its two financial free zones – the Dubai International Free Zone (DIFC) and the Abu Dhabi Global Market (ADGM), which are separate, common law jurisdictions with their own common law courts and financial services regulators. The rest of the territory of the UAE (which for the purposes of this article is referred to as "onshore" UAE is subject to a civil law-based legal system (comprising a mixture of federal and Emirate-specific laws and regulations). Within this complex jurisdictional system, several different approaches to the regulation of crypto and digital assets have emerged and are developing.

Blockchain strategy

In April 2018, the federal government unveiled the Emirates Blockchain Strategy 2021 (EBS), setting out the nation's objective to create a framework and environment where blockchain technology will thrive. The government committed to transporting 50 percent of all government transactions into the blockchain by 2021, which it is estimated to lead to savings of:

- AED 11 billion in transactions and documents processed routinely
- 398 million printed documents annually
- 77 million work hours annually

The EBS was followed by the adoption of the Dubai Blockchain Strategy (DBS), which intended to establish a roadmap for the introduction of blockchain technology for Dubai and the creation of an open platform to share the technology with cities across the globe.

Abu Dhabi Global Market

The Financial Services Regulatory Authority (the financial services regulator of the ADGM) was the first UAE regulator to issue a comprehensive set of rules, guidance, and regulations. For carrying out activities in relation to virtual assets and cryptocurrencies and to introduce a bespoke framework for the regulation of spot virtual asset activities, including those undertaken by multilateral trading facilities, brokers, custodians, asset managers, and other intermediaries.

The new regulatory regime instated rules for the management of risks generally associated with virtual and crypto-asset-related businesses, including those related to market abuse and financial crime, consumer protection, technology governance, custody, and exchange operations.

Dubai International Free Zone

While the ADGM positioned itself as a pioneer in the crypto space, the DIFC, adopted a much more cautious approach. As a first step, in October 2021, following a consultation process, the Dubai Financial Services Authority (DFSA) – the financial services regulator in the DIFC – issued a new regulatory framework relating to investment tokens. In April 2022, the DFSA issued a consultation paper on a proposed regulatory framework for crypto-assets. It is expected that the new regulations will be published in the latter half 2022.

Onshore UAE (federal level)

Within onshore UAE, the responsibility for the regulation of virtual and crypto-assets is divided between the UAE Securities and Commodities Authority (SCA) and the UAE Central Bank (CBUAE).

SCA

The SCA is tasked with regulating crypto-assets, which are deemed to be a product or security.

In 2020, the SCA released its much-anticipated Decision No. 21/R.M of 2020 concerning the Regulation of crypto-assets (the SCA Regulations), which is intended to regulate the offering, issuing, listing, and trading of crypto-assets in onshore UAE, as well as associated financial activities.

The SCA Regulations apply to: (a) any person in the UAE who offers, issues, or promotes crypto-assets; (b) anyone who provides crypto custody services and/or operates a crypto fundraising platform and/or a crypto-asset exchange in the UAE; and (c) anyone who engages in other financial operations in the UAE in relation to crypto-assets (Article 3 of the SCA Regulations).

It does not apply to crypto-assets issued by the government and/or public undertakings, a currency, virtual currency, digital currency, unit of stored value, or any other payment unit issued through a system licensed, approved, and authorized by the Central Bank of the United Emirates (CBUAE) from time to time, and Securities held in dematerialized form that are not issued as crypto-assets.

Central Bank of the United Emirates

All onshore UAE currency-related transactions are regulated by the CBUAE. On September 30, 2020, the CBUAE revamped its regulatory framework applicable to digital payments by issuing the Stored Value Facilities Regulation (Circular No. 6/2020) (the SVF Regulations). The purpose of the SVF Regulations is to create a framework for the operation and regulation of crypto-assets.

Pursuant to the SVF Regulations, the CBUAE may authorize and license companies and organizations in the UAE that issue or provide SVFs, which is defined as "a facility (other than cash) for or in relation to which a Customer, or another person on the Customer's behalf, pays a sum of money (including Money's Worth such as values, reward points, crypto-assets or Virtual Assets) to the issue in exchange for the storage of the value of that money (including Money's Worth)…(Article 1(27) of the SVF Regulations)."

Emirate of Dubai (onshore) – virtual assets regulatory authority

On February 28, 2022, the government of Dubai issued Law No. 4 of 2022 relating to virtual assets (the Virtual Assets Law). This landmark piece of legislation intends to cement the position of Dubai – and the UAE – as a key market for virtual assets and the commercial marketplaces they engender.

The Virtual Assets Law applies to the provision of services relating to virtual assets throughout Dubai, including all of its free zones, except the DIFC. The Virtual Assets Law governs non-fungible tokens, cryptocurrencies, and security tokens.

Notably, the Virtual Assets Law has established Dubai's Virtual Assets Regulatory Authority (VARA). VARA is tasked with providing a full range of services for virtual assets in coordination with the CBUAE and the SCA, including the licensing and regulation of entities carrying out activities in the virtual asset space, development of strategic plans and policies surrounding virtual asset activities, regulating and supervising the issue and offering of virtual assets and tokens, and prescribing regulations in relation to personal data protection and KYC/AML.

VARA is collaborating with its counterparts in various leading jurisdictions, such as the United States, Switzerland, the UK, Singapore, and Hong Kong with the aim of creating an interoperable set of regulations for activities in the metaverse that can be "passported" to any other jurisdiction. The ultimate goal of VARA is to ensure that any company operating under and complying with its regulations in Dubai can obtain recognition as a reliable and stable company in this space globally.

VARA's approach for the short- to medium-term is to identify and support Virtual Asset Service Providers (VASPs) and numerous other companies through its MetaHQ that import dimensions of virtual assets in their strategy. VARA's main goal is to support what it describes as game-changers, innovators, and market makers across ICT, financial and professional services, lifestyle, entertainment, and FMCG sectors, beyond the world of gaming and VASPs.

Numerous projects, initiatives, and developments are already being encouraged as the UAE is positioning to be a leader in the field of metaverse-related laws and regulation.

In the UAE, we can expect to see regulations being adopted, adapted and amended to keep pace with the rapid advance in the world of web3 and innovations in the metaverse. Any company looking to expand into the metaverse will find the UAE a tax-friendly business foundation with a supportive legislative framework.

Authors

Adela Mues
Partner
Dubai
ameus@reedsmith.com

Soham Panchamiya
Associate
Dubai
spanchamiya@reedsmith.com

Deepfakes in the metaverse

Deepfakes take the form of face reenactment (where software manipulates an individual's facial features), face generation (where a new face is created that does not relate to a specific individual), face swapping (where one person's face is swapped with another's), and speech synthesis (where voices are re-created). Shallowfakes are similar, but they involve more basic editing techniques.

How do deepfakes and shallowfakes relate to the metaverse?

By their very nature, deepfakes and shallowfakes are a direct threat to the accuracy of information relating to any individual in the existing digital environment. However, the threat that they pose will only increase as our interactions with the metaverse increase, given that there will be more opportunities for the use of deepfake technology. While many deepfakes have been created as obvious parodies (such as a 2020 deepfake of Richard Nixon announcing the failure of the 1969 Moon landing or the use of deepfakes of Queen Elizabeth II by a UK public service television network in their 2020 "Alternative Christmas Message"), their increasingly convincing nature means that this technology can be used for more troubling purposes. By way of example, in June 2022 it was reported that the mayors of several European capitals had been duped into taking part in video calls with a deepfake of the Mayor of Kyiv, Vitali Klitschko.

What are the legal issues?

Deepfakes and shallowfakes can be used for the manipulation of pornographic material (for example, revenge porn) and for political purposes (for example, to fake political statements or actions). Such uses (which are just two examples among many) can have an obvious and dangerous impact on the privacy and reputation of individuals. This is particularly the case for those in the public eye, but also more widely.

Deepfakes and shallowfakes can be used to suggest that individuals have made comments or taken part in activities (ranging from the controversial or socially unacceptable to the illegal) when they did not. There are also clear implications for the safety of convictions in the criminal justice system.

On the other side of the coin, the existence of such technology allows wrongdoers appearing in unaltered material to claim that it has been altered – again with potential implications for the justice system and the political landscape – potentially allowing wrongdoers to claim that video evidence is "fake news."

There are a number of ways that the law can tackle deepfakes and shallowfakes. For example:

- Revenge porn could be dealt with under the Criminal Justice and Courts Act 2015.
- The Protection from Harassment Act 1997 may be helpful in some cases.
- The owner of the copyright in the footage used may be able to bring an action for copyright infringement (although in many cases, the owner may not be the individual featured). Deepfakes created for comedic purposes may be protected by the parody exception under the Copyright, Designs and Patents Act 1988, relating to any work that "evokes an existing work while being noticeably different from it, and constitutes an expression of humour or mockery."
- Defamation is a potential route in the case of deepfakes that "lower the claimant in the eyes of right-thinking members of society" or cause such members to "shun or avoid" them provided that serious harm is caused. This would be a viable cause of action for more serious deepfakes, such as those wrongly suggesting that individuals in the public eye have made a statement or carried out an activity that might cause serious harm to their reputation.
- Passing off may be helpful, for instance, where a deepfake is used to fake endorsement of a product.
- Privacy law and the tort of misuse of private information may be helpful where footage not intended for public distribution is used, but the fact that most deepfakes are derived from widely available footage may mean that its use is limited.
- If the deepfake is being used in connection with advertising, the affected individual (including a deceased individual) may have a right of publicity claim within the United States. Right of publicity laws vary by state, with some states, such as New York, California, and Tennessee, extending that protection to after death.

In terms of upcoming changes to the law, the European Parliament recently ratified amendments to the draft EU Digital Services Act (due to come into force in 2023) to require "very large online platforms" to label that footage is a deepfake and inauthentic in a "clearly visible" format. It has however been noted that the UK Online Safety Bill does not appear to include equivalent proposals.

Authors

Carolyn Pepper
Partner
London
cpepper@reedsmith.com

Jonathan Andrews
Associate
London
jandrews@reedsmith.com

Managing antitrust and competition risk

In January 2022, the European Commissioner for Competition, Margrethe Vestager, whose responsibilities also include Digital Regulation, was quoted as stating that competition authorities "should start thinking about [the metaverse] now." While almost all competition authorities and legislative bodies around the globe have made digital markets a priority area for enforcement, this call to action is one of the first times that the head of one of the major antitrust authorities has explicitly recognized the need to consider the future of competition enforcement in the metaverse. The emergence of the metaverse and the reinforcement of the ever-increasing pervasiveness of digitization will undoubtedly come under close scrutiny from competition regulators worldwide.

However, to date, there are more questions than answers on how this should be done. Indeed, Ms. Vestager's comments note a concern that developments are occurring that need to be followed, but that the competition authorities are still trying to work out how to ask the right questions to understand potential competition concerns.

- As the world becomes increasingly interconnected, how will competition law enforcers adjust to this trend, and will the individual competition authorities be able to find a way to work together to address issues on a global, rather than a piecemeal, individualized basis?
- At what stage should regulators intervene? If they intervene too soon, innovation could be stifled, and if too late, the market could "tip," causing substantial distortion of competition, risk of monopolization, and emergence of mega-corporations.
- Do regulators have a choice at all of balancing intervention, just in case they risk falling behind rapidly changing digital developments?
- Will the competition tools that have been or are currently being developed to address powerful digital platforms prove to be sufficient, or will they be outdated even before they are effectively applied?
- Will there be a way to provide legal certainty for companies doing business in the metaverse, and will there be guidance that companies can rely on when adapting their business models to the new age?
- What steps should be taken to safeguard consumers in the metaverse jungle?

Even at this early stage, it is possible to identify a number of issues competition authorities across the world will have to grapple with. The competition issues the metaverse is likely to create can be looked at from different perspectives, including

i. the infrastructure needed in the metaverse,

ii. operating a business in the metaverse, and

iii. the roles of users in the metaverse.

Infrastructure needed in the metaverse

Access to the metaverse and gatekeepers – competition authorities will likely want to ensure that there is sufficient access to products or services deemed indispensable for effective competition in digital markets, in particular in the metaverse (for example, access to data, hosting/server capacities, critical technologies or solutions for metaverse-specific types of advertisement, augmented reality/display, etc.).

Standard setting and interoperability – In order for the metaverse to operate effectively, it appears likely that there will need to be agreement on technical standards. We expect regulators will want the metaverse and markets therein to remain open and accessible to market participants (in particular smaller players) on FRAND (fair, reasonable, and non-discriminatory) terms, balanced against the legitimate commercial interests of relevant suppliers to incentivize development and innovation. The tensions between intellectual property holders, licensors of standard essential intellectual property, and licensees that continue to be prevalent in a number of sectors can be expected to arise in the context of the metaverse.

- Merger control and *ex ante* regulation – Today, there is a consensus among competition authorities around the world that *ex ante* regulation (preventing harm to competition before it occurs) is far more effective, less invasive, and thus generally preferred to ex post regulation (retrospective enforcement activity), which tends to entail lengthy administrative proceedings often followed by even lengthier court proceedings. *Ex post* intervention often fails to address the competition issues in the fast-changing digital world in a timely manner. Especially in the digital economy, many markets show a high degree of concentration, and the metaverse is unlikely to change this trend. Furthermore, takeovers and mergers can tip a market or create ecosystems that are almost unassailable for competitors. For this reason, regulators are likely to take merger control more seriously than ever in the context of the new digital era.
- Saving innovation from "killer acquisitions" – Innovating firms are often acquired by incumbents, typically in the early stages of product development and often for large amounts that do not appear to be justified by current revenues. Such acquisitions are referred to as "killer acquisitions" where there is a risk that the purchase of a new challenger by an incumbent will eliminate promising, yet likely competing, innovation. Such acquisitions seem all the more likely to occur in the metaverse, as large digital platforms jostle to position themselves to take advantage of the new technology. Competition authorities are developing tools to enhance pre-merger screenings to discourage these acquisitions when competition is negatively impacted, and the authorities can be expected to vigorously enforce these tools in the context of metaverse M&A.

Doing business in the metaverse

- The overall challenge for regulators will be to keep markets open and free, and to allow companies to do business with consumers in the metaverse. This is always a challenge for competition authorities in times when new "markets" are developing or major developments or innovations occur with the potential to disrupt existing business models.
- Generally, we expect that the rules currently being developed to address market power identified among certain digital companies will continue to be relevant in the context of the metaverse. A number of the issues that have the potential to arise in the metaverse are already being considered in existing digital markets.
- The tendency for markets to "tip" due to the benefits to users and businesses of a critical mass of other users on the same platform can make it very difficult for new competitors to break into the market.
- Users will need some manner to interface with the metaverse. Where this occurs – particularly if there is only a single interface platform or a small number of interface platforms – those platforms have a benefit in being able to favor their own services in secondary markets within the metaverse over services offered by their competitors. Competition authorities consider this type of self-preferencing practice by digital platforms to be potentially harmful as likely distorting competition and increasing dependencies of third-party businesses from the platform's services. This practice can therefore be expected to remain on the "blacklists."
- Advertising markets in digital ecosystems have been the subject of a number of competition investigations in recent years. We expect that competition authorities will continue to take a keen interest in digital advertising in the metaverse, particularly if an advertising-funded business model becomes prevalent.

- The further integration of the digital world with consumers' day-to-day lives will generate huge amounts of data about individuals' routines, habits, and preferences. Access to this data can be vital in ensuring the popularity of services offered in the metaverse. The position of the platform provider can, therefore, impart a significant advantage over rivals, serving to reinforce the platform's market power or enable it to leverage the power to other service areas.

Users in the metaverse

Over recent years, users have become familiar and comfortable with platforms being provided for free at point of use. It seems likely that users will expect digital services in the metaverse to be available on the same basis. However, not being required to pay money does not mean the consumer is not paying anything. Consumers are generally paying for such "free" services with their data. Given the interconnectedness with so many aspects of their lives in the metaverse, this data will be hugely valuable to businesses. There will be a need for higher privacy standards, more transparency, and a simplification of the ways for consumers to agree to or reject the transfer of their data.

This personalized information can be used to create increasingly personalized product and service offerings, which may include setting personalized pricing for different consumers for the same product or service based on what the business knows about that consumer (the strength of their preference for the service, their income, other products they have bought, their location, etc.). Competition authorities have already been considering this issue in digital markets and debating whether exploiting customers' willingness to pay is fair and where the limits of any possible efficiencies will be reached.

In the metaverse, interoperability will set new standards – but not only from the perspective of enabling businesses to connect to the digital platforms. Interoperability will also likely become a standard requirement imposed by competition policy to require digital platforms to provide consumers with the ability to port their data when deciding to leave a platform. Digital platforms are more likely to gather market power if consumers are "locked in" due to the lack of interoperability and the consequence that data is lost when leaving. If consumers are allowed to migrate their data to competing systems (for example, using an application programming interface), lock-in effects would be diminished, which may promote competition between platforms.

Authors

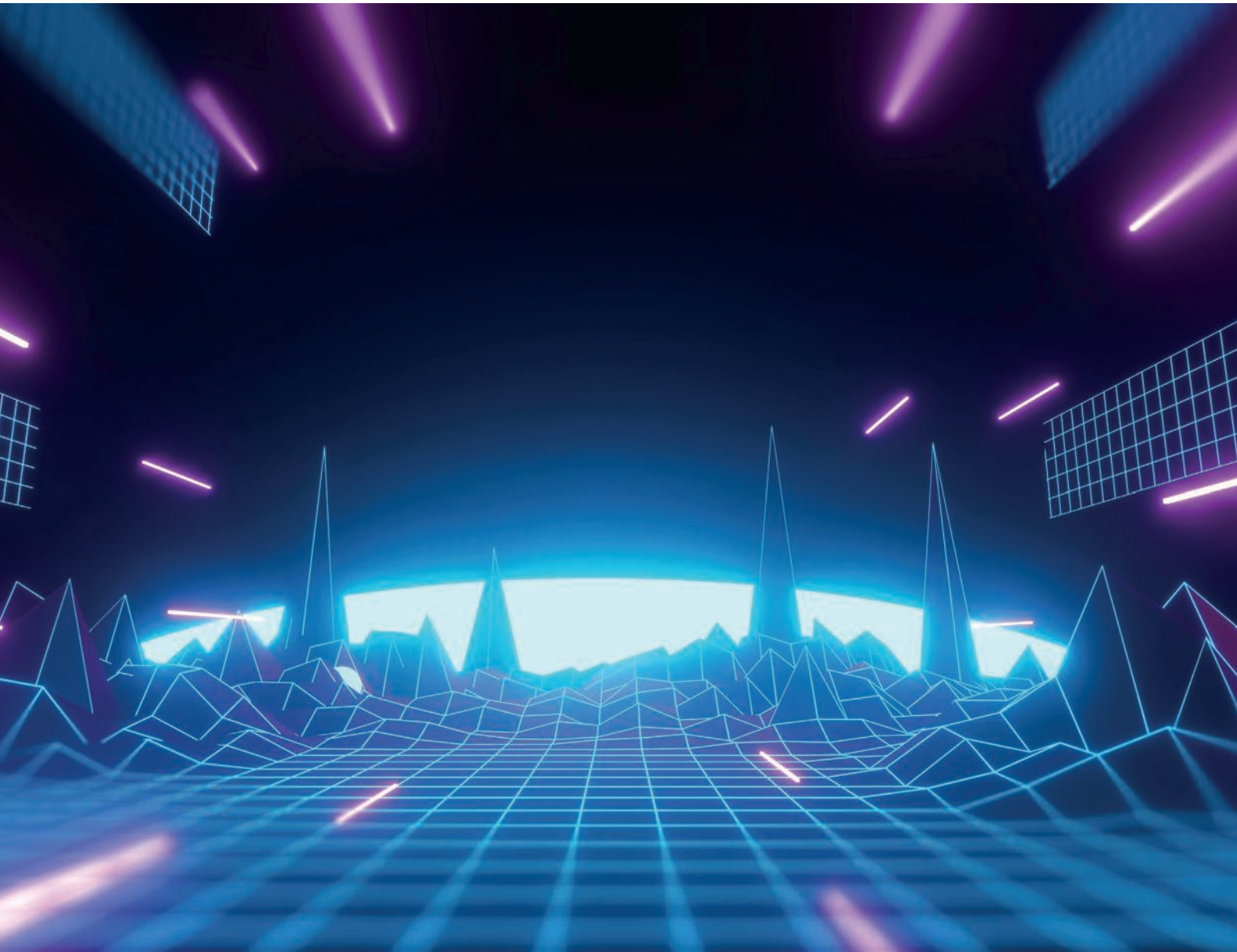
Ross Mackenzie
Legal Consultant
London
rmackenzie@reedsmith.com

Michaela Westrup
Partner
Munich
mwestrup@reedsmith.com

Michelle Mantine
Partner
Pittsburgh
mmantine@reedsmith.com

Aviation in the metaverse: Breaking the reality barrier

Aviation has always been an industry of pioneers, so it comes as no surprise that it has been quick to embrace new technology. The endless possibilities offered by the metaverse are being explored at pace, and the advent of electric vertical take-off and landing (eVTOL) aircraft and unmanned aerial equipment like drones marks the arrival of the next generation of urban air mobility vehicles. At Reed Smith, we have been privileged to play a leading role in the introduction of this transformative technology – albeit a small one in comparison to that of the engineers and entrepreneurs.



Leaving on a jet plane

Aviation was one of the industries most severely impacted by the COVID-19 pandemic, and it remains under pressure from various macro factors: rising interest rates, staff shortages, the price of fuel, and, of course, the increasing replacement of business travel with virtual meetings. Against that backdrop, airlines and airports are turning to the metaverse to augment their offering.

For example, the airport experience has been digitally enhanced with:

- Virtual queuing: trialed at LAX
- Immersive shopping: London's Heathrow Airport partnered with luxury brands like Chanel and their "beauty spaceship," enabling shopping passengers to try on products virtually
- Virtual replicas: Qatar Airways recently launched QVerse, a virtual reality program that allows passengers to look inside the aircraft from the comfort of their homes

Manufacturers are also pushing boundaries via the metaverse, with Airbus and Boeing looking at ways to streamline production by creating digital replicas of aircraft and using these to run tests and simulations. This means they would be able to gather data and results without needing to accumulate flight hours on a physical trial aircraft, saving costs and mitigating safety risks to the test crew. Airbus and HeroX also held a crowdsourcing competition called "Metaverse and the Future of Flight," seeking innovative ways to use the metaverse to reimagine and elevate the traveler experience.

I can see for miles

If the metaverse can facilitate airport access and airport shopping, it can also make it easier to earn and redeem air miles. Many of us are lured by frequent flyer programs that offer benefits with an airline, and these create huge real-world value for both travelers and airlines in addition to generating customer loyalty. Air miles are very lucrative for those airlines that manage to monetize their loyalty programs, which are often worth considerably more than the airline itself. American Airlines, for example, used its program as collateral to borrow money from the U.S. government.

Taking this a step further, airBaltic, the first airline to accept cryptocurrencies in payment for tickets, also became the first airline to issue non-fungible tokens (NFTs) when it launched "Planies," an NFT collection of tokens that it will be linking to its loyalty program. Emirates will also launch NFTs and experiences in the metaverse, alongside both collectible and utility-based NFTs.

Air mile programs are also closely connected with ticket sales, and this new technology offers novel distribution opportunities. Air Europa, for example, has established a partnership with blockchain distribution company TravelX (the company building the first blockchain-based distribution protocol for the travel industry) to come up with the world's first NFT flight ticket series, or "NFTickets," entitling owners to access a special flight to an event in Miami Beach. This will allow passengers to manage and transact with tickets using their own blockchain wallet, combined with a new kind of collectible art piece. At auction, Air Europa's first NFT sold for $1 million. As another example, Vueling is looking to sell flights in the metaverse that can be used in the real world, providing the airline with a new distribution channel.

Learn to fly

Advanced air mobility marks the next inflection point in aviation's continual evolution, and is described by leading industry figures such as Dómhnal Slattery as "the next big frontier" for aviation. It is a frontier being explored by a combination of entrepreneurs, giants of aerospace, and global logistics companies, like Airbus and Boeing (Aurora), Amazon Prime, DHL, and even an online food ordering and delivery service.

eVTOL aircraft in particular represent (among other things) an evolution in the aviation industry's focus as the need to design modes of transportation with substantially lower greenhouse gas emissions and noise pollution becomes ever more urgent. eVTOLs have a wide variety of use cases in both urban and regional areas, and will be used for passenger service, freight, disaster relief, defense, and final mile logistics.

These aircraft are being developed by a range of companies working in this space, but many (if not most) of the proposed models will have to commence commercial passenger operations with a pilot physically on board. It is expected that piloted models will achieve certification in various jurisdictions several years ahead of autonomous aircraft, which is reflective of the need to develop the technology, the regulatory framework, and the passenger buy-in necessary to make this possible. However, the achievement of autonomous flight without a pilot is critical to the ultimate economic viability of eVTOL flight. Consider, for example, a four-seat model of eVTOL aircraft: with a pilot present, the capacity of the aircraft to generate return for its operator (and that operator's financiers) is reduced by 25 percent.

But what if there is an interim stage between piloted and autonomous flight, where the aircraft could be piloted remotely? If the metaverse can be used to build a digital twin of a physical space, the conditions in an eVTOL operating location could be replicated such that a pilot in any location could operate it safely. It might be possible, for example, to overlay a Google Earth-style functionality on top of the virtual replica of the landscape, including marking safe glide paths for use in the event of a malfunction and the "obstacle-free volume" area to be stipulated for each vertiport. This could be supplemented in real time by each vehicle's cameras and other sensors (to deal with, for example, cranes moving over construction sites) and input from passengers.

Taking the pilot out of the payload offers an immediate uplift in return, enabling the same vehicle to carry an additional paying passenger or more revenue-generating cargo and enabling the industry to reach economic sustainability sooner, even before complete autonomy of flight is achieved. Building this support infrastructure in the metaverse could also help address the global pilot shortage, which could be alleviated if the next generation of pilots of eVTOL aircraft could be trained remotely, certified centrally, and deployed globally.

The legal issues

With such complex and novel technology, the range of legal and regulatory obstacles to be considered and addressed by the fledgling eVTOL industry is vast and growing. It will be critical for industry stakeholders to engage with the following topics in particular:

1. Certification: eVTOLs are difficult to define due to the multitude of designs currently being proposed. This makes the task of creating certification standards challenging. Close collaboration with regulators and aviation authorities is obviously therefore essential.

2. Insurances: Industry thinking on the applicable liability issues, and the laws that may regulate accidents and incidents, remain in progress. Recent lessons learned by the insurance community from developments in the unmanned aerial vehicle/drone market have demonstrated that traditional policy wordings are probably not fit for purpose when it comes to insuring new technology such as eVTOLs. This is especially the case if operational infrastructure is built in the metaverse, and new insurance policy wordings accommodating the new technology will need to be developed.

3. Liability and risk allocation: The liability regimes for the carriage of passengers and cargo on board traditional civil aircraft have developed by international convention since commercial flights began in the 1920s, but questions remain as to whether the existing liability framework is flexible enough to accommodate eVTOL flight. Manufacturers and operators will also need to consider how to apportion liability among themselves, as well as the risks that can be passed on to end users via their contractual ticketing arrangements. A careful balance will need to be struck because overly robust indemnity and liability wording could significantly undermine confidence in the industry and would no doubt be met with resistance from regulators and legislators (if not already fettered by consumer protection legislation). It remains to be seen how liability issues in the metaverse more broadly will be addressed, but a single metaverse with multiple stakeholders having different needs, purposes, and levels of sophistication will require carefully designed interoperability standards. In particular, different aircraft manufacturers and vertiport developers will need to permit interoperability between their platforms.
4. Cybersecurity and physical safety: Security and safety issues may arise because of closer operating proximity to potentially malicious actors and to urban public infrastructure. If vehicles can be operated using the metaverse, there is a risk that they could be interfered with in the same way. In addition, both passenger data and flight ops/aircraft-specific data in the metaverse will be extremely valuable, both to bad actors and to marketeers alike.

Aviation is well placed to maximize the potential of the metaverse, particularly in conjunction with emergent technologies like eVTOL aircraft. As these fields develop and overlap, the legal and regulatory frameworks facilitating this potential must evolve quickly and in close collaboration to ensure that aviation is able to benefit from the wealth of new possibilities.

Authors

Richard Hakes
Partner
London
rhakes@reedsmith.com

Ashleigh Standen
Associate
London
astanden@reedsmith.com

Luke Drake
Associate
London
ldrake@reedsmith.com

Celine Collis
Associate
London
ccollins@reedsmith.com

Insurance issues in the metaverse

As more companies and people migrate to the metaverse to conduct business, interact, and spend time, companies need to be prepared for losses and claims that could arise from their presence and activity there. Insurance coverage, including bespoke policies and coverage from policies within a company's existing insurance program, can be vital to protect companies against these potential risks.

Many risks companies face in the real world will exist in the metaverse, albeit with a digital twist. For example, many metaverse projects involving the use of a "currency" feature their own native coins, which in many instances can be swapped for other cryptocurrencies or even fiat currency. These activities and operations may lead to allegations of wrongful acts implicating directors and officers (D&O) or errors and omissions (E&O) coverage, among other types of coverage. Many metaverse projects will feature content creation that could implicate intellectual property rights, thereby triggering these same coverages or, potentially, commercial general liability (CGL) coverage or specialized intellectual property coverage. In the metaverse, people can interact with each other via their avatars and haptic feedback and, in some cases, may be accused of causing emotional distress or other torts through those interactions. Events like that may trigger a variety of liability insurance policies, including, if occurring within the virtual workplace, employment practices liability policies. These examples, and the examples set forth below, are just a sample of the core insurance coverages that could be implicated by risks presented by the metaverse.

D&O insurance

D&O insurance shields a company's board and management and protects their personal assets from liability. It typically insures claims made against (1) the directors and officers when the company does not indemnify them ("Side A" coverage) and (2) the company itself when it is required to indemnify its directors and officers for those claims ("Side B" coverage). D&O policies also can include entity coverage protecting the company against its own liability in a securities claim or (in the case of private companies) any non-excluded claim made against the company ("Side C" coverage). D&O insurance is particularly important because it can cover defense costs and indemnity for a variety of claims and suits, depending on the policy language.

D&O risks presented by the metaverse may include:

- Securities claims
- Intellectual property claims
- Breach of fiduciary duty claims
- Misrepresentation claims
- Shareholder and derivative lawsuits
- Regulatory investigations

An insured must be wary of the specific terms and provisions of their D&O policies. While existing D&O policies likely would cover metaverse-related claims for directors and officers of companies entering the metaverse in the same manner that they cover non-metaverse claims, many insurers deny coverage for cryptocurrency-related losses or issue policies with language severely limiting such coverage. In particular, companies dealing in cryptocurrency should be mindful of the definition of a "Securities Claim." Depending on the policy language and the applicable law of the jurisdiction, a D&O policy may protect a company and/or its management from metaverse-related liability as a "Securities Claim."[10]

Additionally, regulators in the future could investigate metaverse companies for a variety of alleged acts or omissions involving operations, cryptocurrency and non-fungible token (NFT) transactions, user conduct, and privacy and data security, to name just a few. These investigations can be costly. A D&O policy may cover some or all of the costs associated with such an investigation. However, it is important to ensure that the policy does not exclude investigations for cryptocurrency-related activities or the insured's operations in the metaverse.

Cyber and crime

With its increasing adoption, the information stored in the metaverse will entice bad actors who want to steal valuable data and items. Among other things, hackers could target:

- User information and sensitive data (including biometric data)
- User identity information and credentials
- Confidential and proprietary information
- Cryptocurrencies and NFTs

Cyber and crime insurance can mitigate some of these risks. Cyber insurance is designed to provide first- and third-party coverage for claims arising out of security or privacy breaches, such as ransomware attacks or cyber extortion. Depending on the policy language and coverages purchased, cyber insurance may provide coverage for costs of investigation, ransom payments, data recovery and restoration, crisis management, business interruption, and liability claims for disclosure of or failure to protect confidential information.

Similarly, crime coverage may cover losses arising from certain criminal incidents, such as theft of money, securities, or property; ransomware attacks; social engineering; fraud; and phishing, among others. In a recent case in New York, a court examined coverage under an identity theft policy for the theft of private key credentials to an insured's cryptocurrency account and subsequent looting of the insured's cryptocurrency.[11] The court partially sided with the insured, finding that the hack and subsequent theft of the insured's private keys constituted a covered "Stolen Identity Event."[12] The court permitted the insured's stolen key credentials claim to proceed, but held that the insured was not entitled to remediation coverage for its lost cryptocurrency because the private wallet was not an "Account," i.e., an account

10 At the time of writing, it is not clear whether cryptocurrency is a security under U.S. law. In *S.E.C. v. Ripple Labs, Inc., No. 20-cv-10832 (S.D.N.Y. 2020)*, a U.S. federal court is considering arguments from the U.S. Securities and Exchange Commission that Ripple's cryptocurrency, XRP, is a security.

11 *Atwal v. NortonLifeLock, Inc., No. 20-cv-449S, 2022 U.S. Dist. LEXIS 93153 (W.D.N.Y. May 24, 2022).*

12 *Id. at *13-18.*

in a U.S. regulated and domiciled financial institution.[13] The decision demonstrates challenges in obtaining coverage for emerging metaverse-related risks, including crypto.

It is important to note that cyber and crime policies sometimes include language purporting to limit or exclude coverage for cryptocurrency and digital asset-related losses. An insured must be wary of such exclusions and – as is true regarding many risks associated with the metaverse – consider negotiating more favorable terms.

Other considerations

Metaverse projects may involve alternative governance structures, e.g., decentralized autonomous organizations (DAOs). For this reason, nontraditional organizations and companies active in the metaverse must be particularly careful in naming the correct entities as insureds under their policies. In many jurisdictions, DAOs are not legal entities so they may be precluded from purchasing insurance policies and may need to secure insurance through another legal entity structure. Some DAOs have foundations to protect their legal rights (e.g., The Decentraland Foundation), while others may utilize more traditional forms of corporate governance. Either way, a company must ensure that it and its board and management have adequate insurance coverage against risks presented by the metaverse.

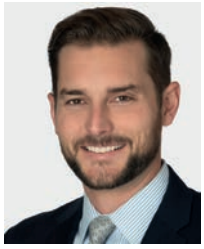
If metaverse-related losses or liabilities arise, companies should take a careful look at their existing insurance programs to see whether coverage may be available. Companies operating in the metaverse should also keep abreast of any new insurance products for metaverse applications, such as specific coverages for digital assets. As this area develops, it is especially important to retain experienced insurance coverage counsel to assist with negotiating and procuring insurance and in navigating any disputes that may arise related to losses and claims.

13 *Id.*

Authors

Noel Paul
Partner
Chicago
npaul@reedsmith.com

Miranda Jannuzzi
Counsel
Philadelphia
mjannuzzi@reedsmith.com



Nick Pappas
Associate
Los Angeles
npappas@reedsmith.com

Phone: +44 (0)20 3116 3000
Fax: +44 (0)20 3116 3999
DX 1066 City/DX18 London

ABU DHABI
ATHENS
AUSTIN
BEIJING
BRUSSELS
CENTURY CITY
CHICAGO
DALLAS
DUBAI
FRANKFURT
HONG KONG
HOUSTON
KAZAKHSTAN
LONDON
LOS ANGELES
MIAMI
MUNICH
NEW YORK
PARIS
PHILADELPHIA
PITTSBURGH
PRINCETON
RICHMOND
SAN FRANCISCO
SHANGHAI
SILICON VALLEY
SINGAPORE
TYSONS
WASHINGTON, D.C.
WILMINGTON

reedsmith.com