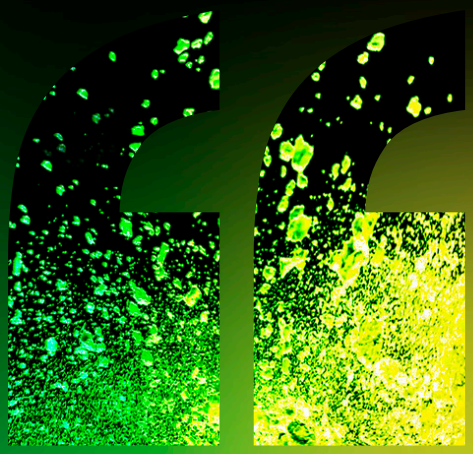
CLIFFORD
CHANCE



THE METAVERSE: RISKS AND OPPORTUNITIES FOR BUSINESSES

— THOUGHT LEADERSHIP

JULY 2022

THE METAVERSE: RISKS AND OPPORTUNITIES FOR BUSINESSES

Companies across a wide range of sectors are exploring the commercial potential of the metaverse but will need to navigate a complex patchwork of existing and emerging laws if they are to successfully operate in these virtual worlds. We examine some of the opportunities and the legal risks that may lie ahead.

1 Digital goods

As a fully virtual environment, the metaverse is a natural home for digital goods. Digital goods are attracting significant investment and attention from brands, with Morgan Stanley predicting the metaverse could be worth US$50 billion dollars for fashion and luxury brands by 2030. Companies are exploring various monetization options and digital-to-physical collaborations, including "digital twins" – selling real products and pairing these with a matching non-fungible token (NFT).

Legal considerations include:

- **Intellectual property protection:** Although the metaverse is not a single place or jurisdiction, brands operating within it should ensure that they have filed the requisite trademarks to protect their use in the metaverse. Care will also be needed in contractual arrangements – companies will need to enter appropriate licensing arrangements that contain ring-fencing provisions to protect their title, rights, and interests in preexisting IP, and will need to ensure that the scope of such license is clearly outlined from the outset – for example, the IP being licensed, field and use, exclusivity, territory, and term of use. Developments involving inclusion of user-generated content, such as submission of user designs, will need to explicitly state in the terms of service that the brand will be granted the rights to publish and display user contributions throughout the world in any media to avoid IP infringement claims from users.
- **Tax:** Companies entering the world of digital goods also need to consider the tax consequences. Whilst the taxation of cryptocurrencies has been addressed in guidance by a number of tax authorities across the globe, the tax treatment of other digital assets, such as NFTs, and which jurisdiction should have taxing rights given their decentralized nature, remains unclear. Currently, determining the correct tax treatment of cryptoassets involves analyzing various aspects of each asset to work out the most appropriate existing tax regime to apply. NFTs and digital twins present particularly tricky questions, such as which asset is being sold: is it a security, or certain limited rights in the underlying asset, or the underlying asset itself?

(See our articles: **NFTs – An Introduction and Some Key Intellectual Property Considerations** and **Non-Fungible Tokens - The Global Legal Impact**.)

2 Virtual lives, physical devices and IoT

Internet of Things (IoT) devices, including virtual reality headsets, augmented reality glasses, smart watches, sensor gloves and smart TVs, will be essential in connecting consumers to the metaverse. As well as presenting opportunities for IoT designers, manufacturers, and distributors, these devices will open up new possibilities for the wider metaverse ecosystem to offer consumers increasingly sophisticated immersive and bespoke experiences and a deeper level of brand engagement.

Companies are likely to be able to understand their customers in a much more intimate way than the traditional internet use allowed, as IoT devices have the ability to record individuals' physiological responses and biometric data such as facial expressions, vocal inflections, and vital signs in real time. Metaverse users may also be "logged in"

for extended periods of time, generating data while they live their virtual lives and thereby potentially "disclosing" far more data than they do through use of the internet today.

Legal considerations include:

- **IoT data use and access:** Connected devices collect and generate an unprecedented amount of data. As well as being mindful of data privacy and security obligations (discussed further below), companies will need to monitor the evolution of the legal framework for the design and use of connected devices and the data they generate. The proposed EU Data Act, for example, will govern accessibility to data (including any non-personal data) generated by using IoT products, with implications for product and system design, contract terms, and data governance frameworks.
- **Privacy:** Although many data protection and privacy laws, such as the EU's General Data Protection Regulation (GDPR), are technologically neutral, the metaverse creates new data privacy challenges due to the volume and range of personal data that could be generated through user engagement. This extends beyond data collected about an individual through a connected device – data relating purely to a device or to an avatar can also fall within the scope of privacy laws if it can ultimately be linked to an individual when combined with other information. Where personal data is processed, requirements on companies can include conducting certain risk assessments, providing notices, identifying appropriate justifications for processing personal data and obtaining consents (where required). Additional challenges can apply to automated decision-making, the processing of specially protected data (such as biometric data, health data, or data revealing racial or ethnic origin), and to the processing of children's data (where consents, notices, age verification techniques and user interface design require particular care). Given the nature of the metaverse and the extra-territorial reach of many privacy and data protection laws, companies will often be navigating these regulations across multiple jurisdictions.
- **Cyber security:** It will also be important to safeguard data appropriately, given that the transfer of sensitive data and virtual payments across platforms heightens the risk of data theft, malware attacks, and data breaches. All online platforms face the challenges of cybersecurity incidents and data breaches, but the breadth and depth of the data collected in the metaverse, including through smart systems which use sensors and monitoring devices in homes, cars, and offices, will make these devices, platforms, and service providers subject to an increased risk of targeted cyberattacks. Cyber incidents pose significant reputational and financial risk to organizations, including substantial potential penalties, disrupted or suspended operations, and a requirement to notify individuals and regulators of certain incidents. In a virtual world with multiple players and flows of data between various platforms, allocation of cyber risk and responsibility will be a key issue.

New ways of marketing

3

The data collection opportunities presented by the metaverse could deepen companies' understanding of their customers' behaviors, enabling more tailored and targeted advertising and personalized interactions, as well as potentially enhancing the user experience.

Many companies are buying virtual real estate in the metaverse to increase brand exposure and benefit from the publicity of being an early entrant. Decentralized platforms offering virtual real estate have seen prices increase dramatically in a relatively short time as banks, celebrities, corporations, and others all acquire space in the metaverse. For many companies it is the marketing budget rather than the investment balance sheet that is fueling these transactions, although there are some interesting concepts developing, including a different type of "digital twin" where virtual

properties and NFTs are used to try and capture information relating to a real building to enhance the real-world operation and efficiency of that physical building.

We are also seeing deep fakes – digitally manipulated images and videos that replace or synthesize images and audio, usually using AI or machine learning – being used in a number of ways by companies, particularly for marketing campaigns. Examples include footballer David Beckham appearing to speak nine languages in a campaign for an anti-malaria charity and the paintings of Salvador Dali coming to life in an immersive exhibition.

Legal considerations include:

- **Evolving regulation of targeted advertising:** Companies will need to keep abreast of developments in laws, guidance, and enforcement appetite in relation to advertising (and particularly targeted advertising). Legal frameworks in this area are under review with new laws on the horizon in various jurisdictions. Examples include the US Banning Surveillance Advertising Bill, the American Data Privacy and Protection Act, the **UK's Online Advertising Programme consultation** on the advertising supply chain, and the **EU Digital Services Act**. There are trends towards increased transparency and control requirements, as well as towards restrictions on targeted advertising to vulnerable groups or using sensitive data. Laws relating to e-Privacy are also evolving, with creation of the **EU e-Privacy Regulations** still in the works and privacy regulators remaining active in relation to certain targeted advertising practices. (See our articles: **Online Advertising Programme – UK Government proposes increased regulatory oversight of online ads**, **The Digital Services Act – what is it and what impact will it have?**, and **E-Privacy check-in: where we are, and where we're headed**.)
- **Virtual real estate:** The phrase "virtual real estate" is an oxymoron. Real estate laws clearly do not apply to these spaces and any investor should look closely at the terms and conditions of the relevant contract before considering whether to invest, particularly as, unlike physical real estate, virtual real estate depends wholly on the vendor for its continued existence. In addition, uncertainty exists around how buying, selling, and leasing digital real estate will be taxed. Physical land, as a finite resource, is often subject to unique tax regimes in the country where the land is situated, but it is still unclear whether (and if so, how) these regimes may be transferred across to digital real estate.
- **Digital events:** An increasing number of companies are offering immersive digital events. Certain gaming companies, for example, are now offering in-game concerts. These digital events give rise to interesting tax questions, in particular around VAT. The current legal framework is not set up to deal with digital events as, for example, current EU VAT rules specifically tax admission to events where the event takes place. Legislators are attempting to tackle this head on, with the EU proposing new rules last year that, if implemented, will mean that virtual events will no longer be deemed to be supplied in the country where the event takes place, but instead in the country of the attendee.
- **AI and transparency:** Deep fakes will be regulated. For example, the draft EU Artificial Intelligence Act (EU AI Act) proposes to impose transparency obligations that will mean deep fakes need to be disclosed to users. It defines deep fakes, broadly, as any AI system that generates or manipulates image, audio, or video content that appreciably resembles existing persons, objects, or places and would falsely appear to someone as authentic or truthful. Like the EU's GDPR, the EU AI Act will apply to some organizations based entirely outside of the EU. Metaverse

spaces will need to be designed carefully and consideration should be given to how these transparency obligations would work in practice, taking into account user experience alongside the ethical and legal ramifications of improper disclosure. (See our briefing: **The future of AI regulation in Europe and its global impact**.)

M&A, investments, and collaborations

4

The success of the metaverse, in whatever form it takes, will require significant investments that will be realised through a combination of organic growth and acquisitions. These will span the full range of digital content, digital assets, hardware, and software needed to generate virtual spaces – for example, with next generation microchips and graphics processors required to render the virtual worlds of the metaverse. Equally important will be the investment required in low-latency and high-bandwidth connectivity infrastructure (such as fiber optics, advanced wireless networks, and 'edge' data centers) needed to connect users and complex virtual worlds in real time.

Corporates and venture capital investors have been setting up funds, collaborations or acquiring minority stakes across the metaverse ecosystem as a way to diversify their core businesses and build a pipeline of possible acquisition targets. Notably, venture investments have poured into the gaming sector, with more than US$10 billion raised in 2021 across gaming, augmented reality, and virtual worlds, and metaverse M&A activity in early 2022 has seen a particular emphasis on acquisitions of gaming IP as well as the valuable communities that go with it.

Faced with exponentially increasing bandwidth consumption and the demand for high-performance connectivity, providers of connectivity infrastructure are already seeking investment and innovation opportunities, including through the formation of joint ventures with financial investors and the establishment of stand-alone technology and cloud-services divisions.

Legal considerations include:

- **Antitrust:** Attempts to build the metaverse through acquisitions, joint ventures, and other partnerships, are likely to attract close antitrust scrutiny. This is due to criticism in various jurisdictions that competition authorities failed to challenge transactions by large tech companies that were anticompetitive (or, in some jurisdictions, lacked the statutory authority to challenge anticompetitive transactions). Antitrust authorities will want to ensure that they do not make the same mistake with what many see as the next iteration of the internet. Additionally, some jurisdictions have implemented or are considering ex-ante antitrust legislation (e.g., the **EU Digital Markets Act (DMA)** or the **American Innovation and Choice Online Act**). Although such legislation would target large technology companies ("gatekeepers" for the DMA or "covered platforms" for the American Innovation and Choice Online Act), such legislation, where enacted, will also impact digital economies more broadly. (See our article: **The Digital Markets Act: A new era for the digital sector in the EU**.)
- **Other transaction notification requirements:** Companies may also need to navigate other regimes which allow governments or regulators to scrutinize and intervene in acquisitions and investments, and which may include notification requirements. For example, the UK's National Security and Investment Act 2021 allows the UK government to call-in, review, and potentially block certain acquisitions and investments in sensitive sectors which could impact national security.

- **Tech M&A due diligence and contracts:** Technology-heavy transactions will require tailored due diligence and contracting processes which are alive to the particular risks and value drivers of the acquisition or investment. What data and intellectual property rights does the target business have (and need), and how is it entitled to use these in light of, for example, third party licenses and data privacy and localization laws? What is the level of cyber risk exposure, and are there any parental liability issues? How are employee and founder incentives aligned, and will their rights impact future options? How will the political and execution risks that come from controls on tech-related foreign investment be managed? How will the transitional delivery of crucial services be managed to ensure the value of the transaction is maintained?

Building the metaverse – interoperability and design

Achieving the full potential of the metaverse relies on sophisticated user interface and seamless interoperability. Creating an immersive, engaging, and responsive environment will involve processing huge amounts of information and is likely to involve the application of machine learning or AI. Behind the scenes, establishing portability and free flow of data and digital assets between applications and platforms in the metaverse according to user preferences will be crucial. Allowing users to navigate virtual spaces seamlessly and move their digital goods and avatars between spaces and applications – even if those platforms and assets are owned or operated by different companies – will be what transforms discrete platforms into a single metaverse. This level of interoperability will need coordination and is likely to involve the development of codes, protocols, or industry standards. Those with early involvement in the building of the metaverse – from development of interfaces and practices to establishment of infrastructure – could shape the future.

Legal considerations include:

- **Antitrust:** While industry standard-setting generally has procompetitive benefits, collaboration among competitors and industry participants can attract antitrust scrutiny. One potential antitrust issue with standard setting, particularly within the context of trade associations, is the risk that a group of companies will adopt a standard that excludes or discriminates against rivals.
- **Portability:** As data portability between metaverse spaces improves, software developers, operators, and brands will need to cooperate more fully, requiring bilateral or multilateral data sharing agreements to improve the seamlessness of the consumer experience. Some laws will impose specific data portability requirements, such as the GDPR and, likely, the proposed **EU Data Act**. Again, data privacy considerations will be important as increasingly strict rules on international data transfers and the global trend of "data localization" laws could make compliance more challenging. (See our article: **The Data Act: A proposed new framework for data access and porting within the EU**.)
- **Privacy responsibility allocation:** A range of other legal questions arise in relation to who will be responsible for complying with applicable data protection laws. It may be difficult to establish which entity has responsibility for determining how and why personal data will be collected and processed. Will different entities be required to display their own privacy notice to users, or will this be done jointly? Who is responsible if users' personal data is stolen or misused while they are in the metaverse? As opposed to the relatively simple "one-on-one" fiction presumed by certain laws, answering these questions may be more difficult within a complex web of multiple decentralized parties operating in the metaverse.

- **Bias, discrimination, and "dark patterns":** Laws that are being introduced to tackle issues evident in our current digital environment will impact design and governance processes for companies shaping the metaverse. For example, the proposed EU AI Act intends to completely prohibit certain AI practices on a risk-graded bases, with areas of focus being subliminal techniques with potential for harm, and prevention of bias and discrimination. Other laws, such as the proposed EU Digital Services Act will also regulate online interface design, particularly "dark patterns" which could distort or impair a user's ability to make informed decisions. Product development teams and marketing departments will need to operate within guardrails set by these emerging requirements to bring these virtual spaces to life in a fair, inclusive, and transparent way.

What's next?

Beyond the hype, the metaverse offers opportunities for organizations across all industries. While it will take years to shape the metaverse or metaverses, front-runners are already making an impact and reaping benefits. As developments unfold in the metaverse, companies will also need to navigate legal challenges and regulatory scrutiny, particularly with respect to data governance, antitrust, tax, responsible design, and IP issues.

CONTACTS

EMEA

Abigail Cessna
Associate
London
T: +44 207006 3366
E: abigail.cessna@cliffordchance.com

Herbert Swaniker
Senior Associate
London
T: +44 207006 6215
E: herbert.swaniker@cliffordchance.com

Jamie Andrew
Senior Associate
London
T: +44 207006 1367
E: jamie.andrew@cliffordchance.com

Uche Eseonu
Lawyer
London
T: +44 207006 6188
E: uche.eseonu@cliffordchance.com

Nicola Hemsley
Partner
London
T: +44 207006 4215
E: nicola.hemsley@cliffordchance.com

Rita Flakoll
Senior Associate
Knowledge Lawyer
London
T: +44 207006 1826
E: rita.flakoll@cliffordchance.com

Chris Grey
Senior Associate
London
T: +44 207006 4984
E: chris.grey@cliffordchance.com

James Law
Senior Associate
London
T: +44 207006 3066
E: james.law@cliffordchance.com

Mark Fisher
Senior Associate
London
T: +44 207006 1480
E: mark.fisher@cliffordchance.com

Arun Visweswaran
Senior Associate
Dubai
T: +971 4503 2748
E: arun.visweswaran@cliffordchance.com

Jonathan Kewley
Partner
London
T: +44 207006 3629
E: jonathan.kewley@cliffordchance.com

Jennifer Mbaluto
Partner
London
T: +44 207006 2932
E: jennifer.mbaluto@cliffordchance.com

Dessislava Savova
Partner
Paris
T: +33 1 4405 5483
E: dessislava.savova@cliffordchance.com

Claudia Milbradt
Partner
Düsseldorf
T: +49 211 4355 5962
E: claudia.milbradt@cliffordchance.com

Josep Montefusco
Partner
Barcelona
T: +34 93 344 2225
E: josep.montefusco@cliffordchance.com

Vanessa Marsland
Partner
London
T: +44 207006 4503
E: vanessa.marsland@cliffordchance.com

Andrea Tuninetti Ferrari
Lawyer - Counsel
Milan
T: +39 02 8063 4435
E: andrea.tuninettiferrari@cliffordchance.com

US

Brian Yin
Associate
New York
T: +1 212 878 4980
E: brian.yin@cliffordchance.com

Timothy Lyons
Associate
Washington DC
T: +1 202 912 5910
E: timothy.lyons@cliffordchance.com

Thomas Chapman
Associate
Washington DC
T: +1 202 912 5921
E: thomas.chapman@cliffordchance.com

Devika Kornbacher
Partner
New York
T: +1 212 878 3424
E: devika.kornbacher@cliffordchance.com

Megan Gordon
Partner
Washington DC
T: +1 202 912 5021
E: megan.gordon@cliffordchance.com

Sharis Pozen
Partner
Washington DC
T: +1 202 912 5226
E: sharis.pozen@cliffordchance.com

Katerina Papacosma
Associate
New York
T: +1 212 878 8136
E: katerina.papacosma@cliffordchance.com

APAC

Paul Landless
Partner
Singapore
T: +65 6410 2235
E: paul.landless@cliffordchance.com

Angelina Gomez
Counsel
Perth
T: +61 8 9262 5521
E: angelina.gomez@cliffordchance.com

Brian Harley
Consultant
Hong Kong
T: +852 2826 2412
E: brian.harley@cliffordchance.com

Rocky Mui
Partner
Hong Kong
T: +852 2826 3481
E: rocky.mui@cliffordchance.com

Natsuko Sugihara
Partner
Tokyo
T: +81 3 6632 6681
E: natsuko.sugihara@cliffordchance.com

Ling Ho
Partner
Hong Kong
T: +852 2826 3479
E: ling.ho@cliffordchance.com

Ella Keating, **Sophie Nannetti** and **Julia Ganis** contributed to the writing of this paper.

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

2207-001814