NORTON ROSE FULBRIGHT

Navigating the metaverse: A global legal and regulatory guide

Part 4: Decentralised models and data issues

Introduction

In the space of a very short time, businesses are focusing on what the metaverse means for them. In addition to commercialising the opportunities available to them, such as new channels to market and enhanced customer engagement, businesses will need to understand and address the associated risks.

Such matters are extremely important for businesses, consumers, law-makers and lawyers alike. In this seven-part guide we consider the following key legal and regulatory issues in relation to the metaverse:

Part 1

What is the metaverse?

Who are the current big players building it?

What will the metaverse mean for business?

What are key technical, operational and governance considerations?

Part 2

Intellectual property and the metaverse

What are virtual reality worlds and virtual items?

Non-fungible tokens

How do traditional IP concepts sit with non-fungible tokens and other works in the metaverse?

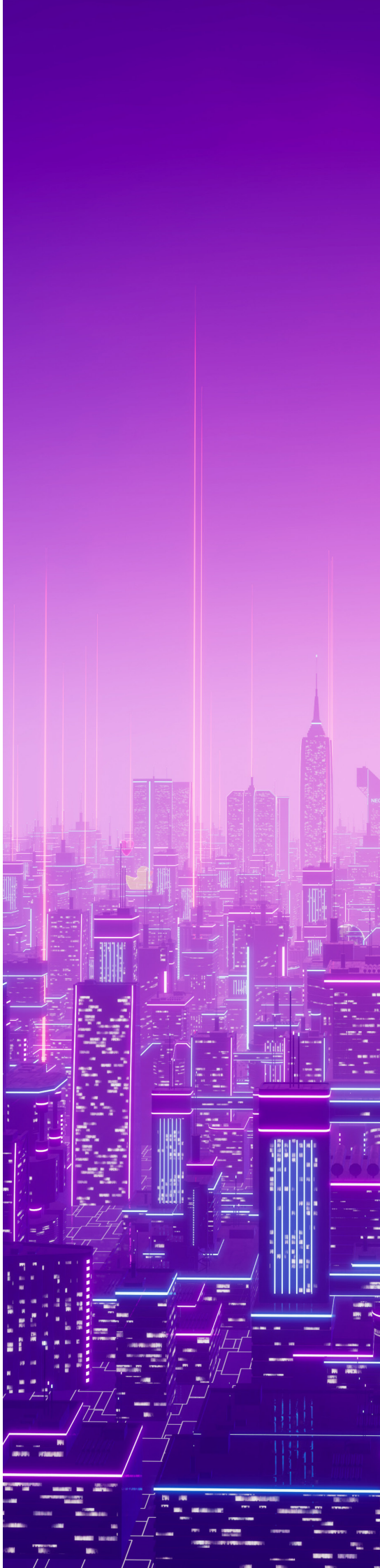
Part 3

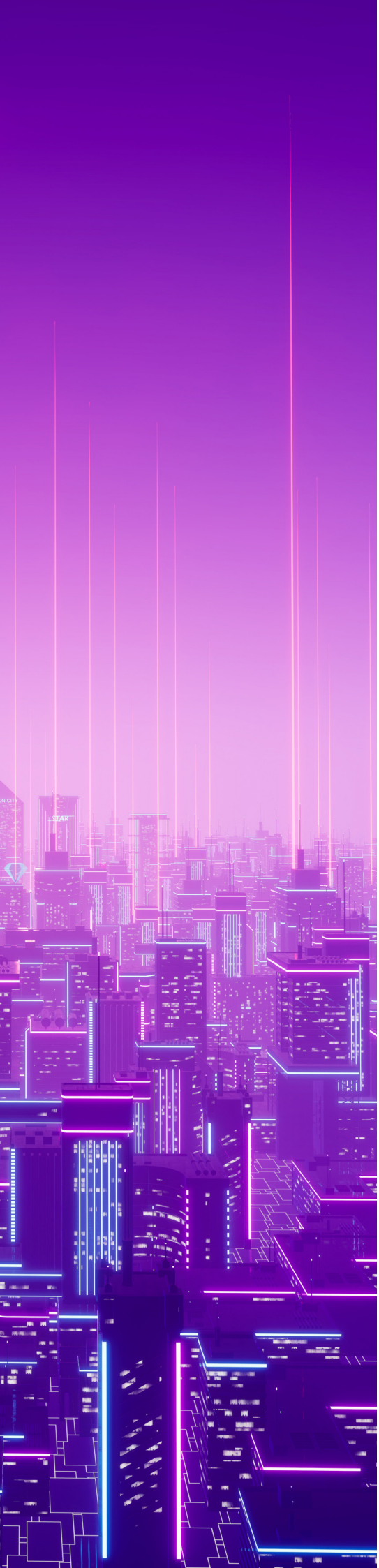
Anti-trust/competition law issues

Developer and participant conduct

Will the EU Digital Markets Act apply to the metaverse?

Competitors communicating and co-operating with each other in relation to metaverse offerings





Part 4

Decentralised models and data issues

Data in the metaverse

Decentralised networks

Who is responsible for data protection law compliance?

Data subject consents

Special categories of data

Children and the metaverse

Data sharing

Data export and localisation

Responsibility for data breaches and cyber attacks

Part 5

Transacting in the metaverse

Buying "land" in the metaverse

What are the key issues when contracting in the metaverse ecosystem?

Non-fungible tokens, smart contracts and blockchain

Financial crime

Will metaverse risk and control considerations be similar to those relevant to the Internet?

Part 6

Digital marketing, adverting and social media in the metaverse

How will businesses be able to advertise in the metaverse?

Social media regulation

Regulating advertising content in the metaverse

Will AI have implications for marketing and the use of avatars in the metaverse?

Part 7

AI and the metaverse

Why is AI relevant to the metaverse?

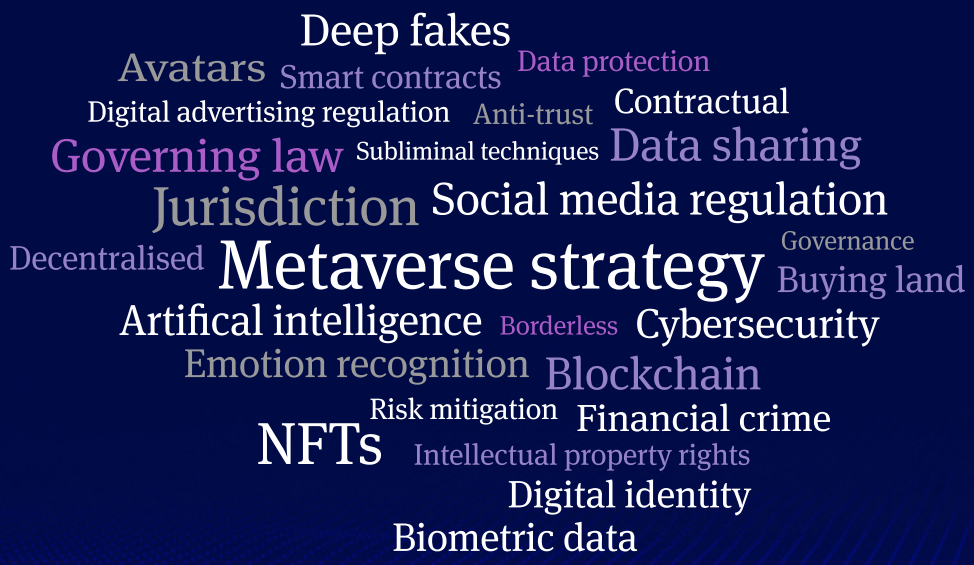
How might AI regulation impact upon the metaverse?

How to operationalise AI risk mitigation in the metaverse

Data protection and AI

Overview of the legal and regulatory issues

The diagram shows the key legal issues and subject areas this guide covers. The breadth of issues means that mitigating risk associated with the metaverse is going to be a significant challenge for any business, but particularly so for a regulated business.



Decentralised models and data issues

Data in the metaverse

Participation in the metaverse will involve the collection of unprecedented amounts and types of data, including personal data. Today's smartphone apps and websites already allow organisations to understand how individuals move around the web or navigate an app. The metaverse will allow the collection of this type of information and much more.

In the metaverse:

- Organisations will be also able to collect information about individuals' physiological responses to content in the metaverse, thereby obtaining a much deeper understanding of their customers' thought processes and behaviours.
- A user will no longer need to proactively provide personal data by opening up their smartphone and accessing their webpage or app of choice. Instead, their data will be gathered in the background while they go about their virtual lives.

It is also anticipated that users participating in the metaverse will be "logged in" for extended amounts of time. This will mean that patterns of behaviour will be continually monitored, enabling the metaverse and the businesses (vendors of goods and services) participating in the metaverse to gather a deeper understanding of their customer-base's preferences and to target those customers in a more targeted way.

Taking some examples:

- The metaverse may observe a user frequently glancing at café and restaurant windows, stopping to look at cakes in a bakery window. Based on that information, the metaverse may determine that the user is hungry and provide advertisements for real-world food delivery services.
- An individual heading to a store in the metaverse might be shown deals on his/her favourite products in real time as he/she is browsing the shelves based on his/her previous behaviour.

Decentralised networks

Applying a legal analysis to such scenarios is complicated by the fact that we may not be talking about one "metaverse" run by a single provider, but a decentralised network of multiple "metaverses" with different platform providers.

If the metaverse operates on a decentralised model, users will likely be moving between various different metaverse platforms in a seamless manner. This will require data sharing between the different platforms to give users that continuity of user experience.

Such data sharing could be seen as being for customer convenience. A user would expect their avatar to have the same look in different metaverse environments without having to register and re-design their avatar each time they move to another platform.

Customer convenience as a driver for sharing data may extend to some sensitive information. For example, the user's credit card details entered on platform 1 would be shared with platform 2 when they change platforms so the customer does not need to enter that information again when they make a purchase on platform 2.

This level of data sharing could also assist in customer targeting. For example, information about our hungry user's behaviour on platform 1 could be shared with platform 2 so that they can continue to be targeted for food delivery services when they enter platform 2.

There are some very real-world issues relating to who "owns" the customer whose data is being shared between different metaverse platforms and metaverse vendors. For example, there may be commercial incentives for some stakeholders to limit the information they are willing to share so that they retain "ownership" of the customer, and managing the expectations and potentially competing interests of all stakeholders will be difficult.

In addition, businesses participating in the metaverse will need to comply with data protection legislation when processing and sharing personal data relating to customers or prospects in this new environment. The international nature of the metaverse further increases the complexity around how that compliance will be achieved in practice.

Who is responsible for data protection law compliance?

Who is going to be responsible for ensuring compliance with data protection legislation in the metaverse? It is a simple question but the answer is potentially quite complicated. In many jurisdictions, data protection laws place different obligations on entities depending on whether an entity determines the purpose and means of processing personal data (referred to as a "controller" under the EU General Data Protection Regulation or GDPR) or whether the entity just processes personal data on behalf of others (referred to as a "processor" under the GDPR).

In the metaverse, establishing which entity or entities have responsibility for determining how and why personal data will be processed, and who processes personal data on behalf of another, may not be easy. It will likely involve picking apart a tangled web of relationships, and there may be no obvious or clear answers – for example:

- Will there be one main administrator of the metaverse who collects all personal data provided within it and determines how that personal data will be processed and shared?
- Alternatively, will multiple entities collect personal data through the metaverse with each determining their own purposes for doing so?

Either way, many questions arise, including:

- How should the different entities display their own privacy notice to users?
- Should each entity do this themselves or should this be done jointly?
- How and when should users' consent be collected?
- Who is responsible if users' personal data is stolen or misused while they are in the metaverse?
- What data sharing arrangements need to be put in place and how will these be implemented?

Data subject consents

Data subject consents are central to how personal data protection laws typically operate around the world. Would a general consent given by the user when they first log into the metaverse to receive marketing materials in the metaverse be sufficient? In many cases, no.

A key driver in the development of the metaverse is its potential to enable new forms of marketing which are seamlessly integrated into the fabric of the metaverse. In our two examples of metaverse marketing set out above (the "hungry user" being given advertisements for real-world food delivery services; or the user being given targeted offers as they browse a metaverse shop), the activity is likely to constitute direct marketing under many countries' data protection laws, which could require the consent of the metaverse user.

The precise nature of the obligations for marketing consents would likely depend on whether the brands themselves instigate the marketing and how the marketing is presented, for example, whether it is akin to targeted ads on a website or marketing sent via some sort of messaging or chat functionality.

However, in all cases, thought needs to be given as to how and when any required data subject consent would be collected and, in particular, whether real-world consent can be relied on by brands in the metaverse and vice versa.

Special categories of data

The use cases for the metaverse typically refer to types of data that might be considered "biometric data", such as records of eye and body movements. Virtual reality headsets and glasses will likely be commonplace in the metaverse unless they are replaced by something more sophisticated in the meantime, such as direct electronic/brain interfaces. Such devices have the potential to collect a wide range of sensitive data about the wearer, including biometric data.

To the extent that such biometric data is used by actors in the metaverse to learn about the user or to make decisions about them, then it will be considered to be special category data under some data protection laws, such as the GDPR. This means that additional regulatory conditions would apply. For example, the user would most likely need to give their explicit consent for each purpose for which the data is used.

In the context of the hungry woman example described above, if the woman were targeted with food advertisements using gaze analysis technology, she would likely have needed to have given her *express* permission to the use of her biometric data for advertising purposes. Depending on the relevant jurisdiction, a general marketing consent may not suffice. Quite how this consent would be sought and given remains to be seen.

It is worth noting that some regulators are starting specifically to consider the collection of this type of sensitive and intrusive data. For example, in its December 2022 "Tech Horizons Report", the UK ICO lists "immersive technology" (including AR and VR technology) as one of the technologies that have the most novel implications for data protection and stresses the need to ensure that such technology is designed and implemented in a privacy positive manner given the privacy challenges and risks that they pose.

Children and the metaverse

A complicating factor in relation to the particular types of data that may be collected in the metaverse is the collection of data relating to children. It is one thing to process personal data of adults in the metaverse, but it is quite another where children are concerned. Many countries' data protection laws provide special protection for children's personal data, and data protection authorities and other similar regulators often come down particularly hard on organisations that do not comply with the rules.

In many circumstances, parental consent is required if a child is to participate in an online service, and to take the EU as an example, the GDPR explicitly states that specific protection is required where children's personal data are used for marketing purposes or creating personality or user profiles.

Sophisticated age verification techniques, enforcing age restrictions and implementing measures to deter children from providing their personal data are therefore going to be essential components of increasing data protection compliance in the metaverse.

Data sharing

In a decentralised metaverse, we have already noted that the platforms may wish to share data between them in order to create a "seamless" experience for users. However, metaverse platform operators may also be sharing information with *other participants* in the ecosystem, like a brand operating a store in the metaverse.

There are already established processes that facilitate data sharing for commercial purposes, including sharing of data across national borders, and the metaverse platform providers and participating brands are going to have to come up with an approach that meets those regulatory requirements in the new context of the metaverse.

For example, one requirement under many data protection laws is that the receiving party's privacy notice must be provided to an individual shortly after it receives the data to explain to the individual how their personal data will be processed. These conditions will become increasingly difficult to meet in the metaverse, where data exchange is rapid and involves a multitude of participants.

One solution to this might be for a central administrator of the metaverse to give users a clear description of how their data will be used and (if necessary) the opportunity to give consent for various uses. However, some data protection regulators have expressed distaste for this type of "catch-all", bundled approach. There may also be a reluctance for the central administrator to take on contractual responsibility for each of the participants' compliance with their regulatory obligations.

Data export and localisation

Issues relating to data export are likely to arise due to the international scope of the metaverse, with data being collected and processed in different jurisdictions. "Seamlessness" in the metaverse demands that data crosses boundaries at speed and without friction. It will be challenging for organisations and/or central metaverse administrators to manage this in the context of the rules around data export and localisation, which are becoming increasingly strict globally.

Responsibility for data breaches and cyber attacks

With so much information being generated and shared in the metaverse and some of that data being particularly sensitive, who is going to be responsible for ensuring the security of data?

As with any online platform, the metaverse will face the usual challenges of fending off cybersecurity incidents and data breaches. However, in the metaverse these types of attacks may also take more "sci-fi" type forms through deep fakes and hacked avatars.

These types of incidents may therefore be harder to identify, verify and bring under control, and it may also be difficult to ascertain where responsibilities lie in respect of breach notification to users and data protection authorities, given the complex web of relationships that entangle the metaverse.

Metaverse user expectations

In addition to complying with data protection requirements, businesses will need to take account of user expectations in relation to the metaverse. For example:

- Who would metaverse users expect to be responsible for protecting the privacy and security of their data as they navigate the metaverse?
- How might user expectations for the metaverse be different from their expectations when they browse the Internet?
- What level of interruption to their user experience will metaverse users tolerate?

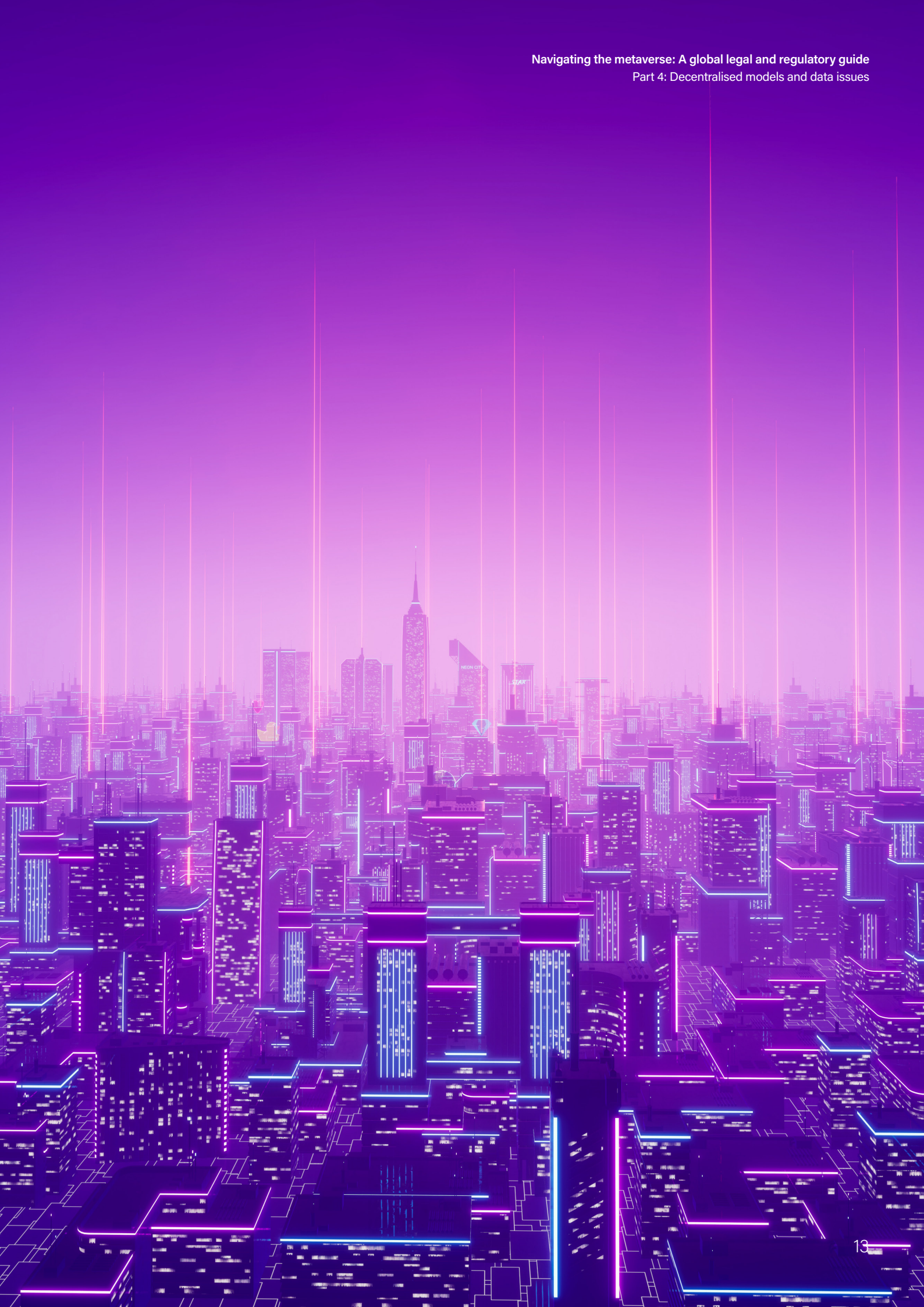
Just like collection of information over the Internet, a key issue will be transparency in how the user's data is being collected and used and facilitating a user's choices to the extent it is technically feasible to do so.

It is unlikely that users will be interested in "swatting away" multiple data privacy notices as they navigate the metaverse. Indeed, regulators could view such practices as actually undermining the requirement to process data transparently, given that users are unlikely ever to engage with the information they are swatting away. Therefore, metaverse participants will need to find solutions that balance the users' legitimate data privacy expectations without detracting from the overall user experience.

As to whom users would expect to be responsible for protection of their data, that answer is more complicated than just naming a single participant in the metaverse environment. Users would expect the metaverse platform provider to have some responsibility for the data sharing ecosystem that they have created, but users may well be sophisticated enough to see that the brand participants are not entirely in the metaverse platform provider's control and that the brand participants should be responsible for their own data handling practices.

Users might expect the metaverse platform provider to take responsibility if they have created a data sharing ecosystem that did not have adequate rules to protect user data (a "metaverse wild west"), but it is possible that they would not expect the metaverse platform provider to be responsible for misuse by a participating brand in breach of the metaverse platform provider's rules.

User expectations do not, of course, trump regulatory requirements, but they are a factor that a business will wish to take into account in considering its own reputational risk when participating in the metaverse.



Key contacts

Australia

Nick Abrahams
Global Co-leader, Digital Transformation Practice
Tel +61 2 9330 8312
nick.abrahams@nortonrosefulbright.com

Ross Phillipson
Senior Advisor
Tel +61 8 6212 3449
ross.phillipson@nortonrosefulbright.com

Belgium

Jay Modrall
Senior Counsel
Tel +32 2 237 61 47
jay.modrall@nortonrosefulbright.com

Canada

Maya Medeiros
Partner
Tel +1 604 641 4846
maya.medeiros@nortonrosefulbright.com

France

Nadège Martin
Partner
Tel +33 1 56 59 53 74
nadege.martin@nortonrosefulbright.com

Clement Monnet
Counsel
Tel +33 1 56 59 53 91
clement.monnet@nortonrosefulbright.com

Sébastien Praicheux
Partner
Tel +33 1 56 59 54 25
sebastien.praicheux@nortonrosefulbright.com

Geoffroy Coulouvrat
Senior Associate
Tel +33 1 56 59 52 98
geoffroy.coulouvrat@nortonrosefulbright.com

Germany

Daniel Marschollek
Partner
Tel +49 69 505096 215
daniel.marschollek@nortonrosefulbright.com

Christoph Ritzer
Partner
Tel +49 69 505096 241
christoph.ritzer@nortonrosefulbright.com

Hong Kong

Justin Davidson
Partner
Tel +852 3405 2426
justin.davidson@nortonrosefulbright.com

Japan

Sam Inohara
Partner
Tel +813 4545 3213
sam.inohara@nortonrosefulbright.com

The Netherlands

Nikolai de Koning
Counsel
Tel +31 20 462 9407
nikolai.dekoning@nortonrosefulbright.com

United Arab Emirates

Adjou Ait Ben Idir
Partner
Tel +971 4 369 6393
adjou.aitbenidir@nortonrosefulbright.com

United States

Felicia J. Boyd
Head of IP Brands, United States
Tel +1 612 321 2206
felicia.boyd@nortonrosefulbright.com

Sean Christy
Partner
Tel +1 404 443 2146
sean.christy@nortonrosefulbright.com

Chuck Hollis
Partner
Tel +1 404 443 2147
chuck.hollis@nortonrosefulbright.com

Andrew Lom
Global Head of Private Wealth
Tel +1 212 318 3119
andrew.lom@nortonrosefulbright.com

Daniel Farris
Partner-in-Charge, Chicago
Tel +1 312 964 7730
daniel.farris@nortonrosefulbright.com

Susan Ross
Counsel
Tel +1 212 318 3280
susan.ross@nortonrosefulbright.com

Robert A. Schwinger
Partner
Tel +1 212 408 5364
robert.schwinger@nortonrosefulbright.com

Rachael Browndorf
Senior Associate
Tel +1 303 801 2763
rachael.browndorf@nortonrosefulbright.com

United Kingdom

James Russell
Partner
Tel +44 20 7444 3902
james.russell@nortonrosefulbright.com

Marcus Evans
EMEA Head of Information Governance, Privacy and Cybersecurity
Tel +44 20 7444 3959
marcus.evans@nortonrosefulbright.com

Lara White
Partner
Tel +44 20 7444 5158
lara.white@nortonrosefulbright.com

Sean Murphy
Global Head of FinTech
Tel +44 20 7444 5039
sean.murphy@nortonrosefulbright.com

Mike Knapper
Head of Intellectual Property, EMEA
Tel +44 20 7444 3998
mike.knapper@nortonrosefulbright.com

Harriet Jones-Fenleigh
Partner
Tel +44 20 7444 2867
harriet.jones-fenleigh@nortonrosefulbright.com

Michael Sinclair
Knowledge Director, Campaigns
Tel +44 20 7444 2344
michael.sinclair@nortonrosefulbright.com

NORTON ROSE FULBRIGHT

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 3500 lawyers and other legal staff based in Europe, the United States, Canada, Latin America, Asia, Australia, Africa and the Middle East.

Law around the world

nortonrosefulbright.com

50962_EMEA – 09/23