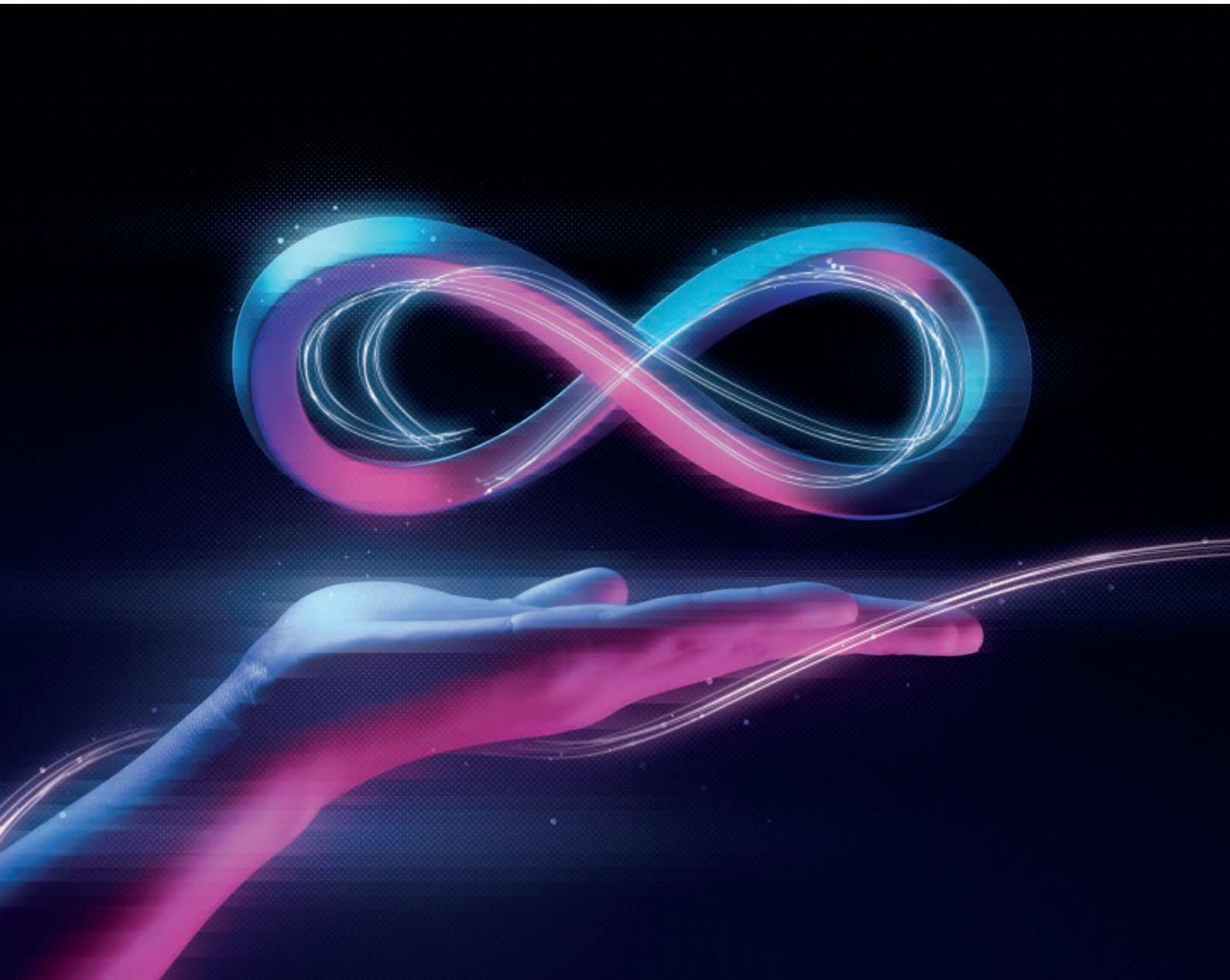
Data protection and privacy

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.

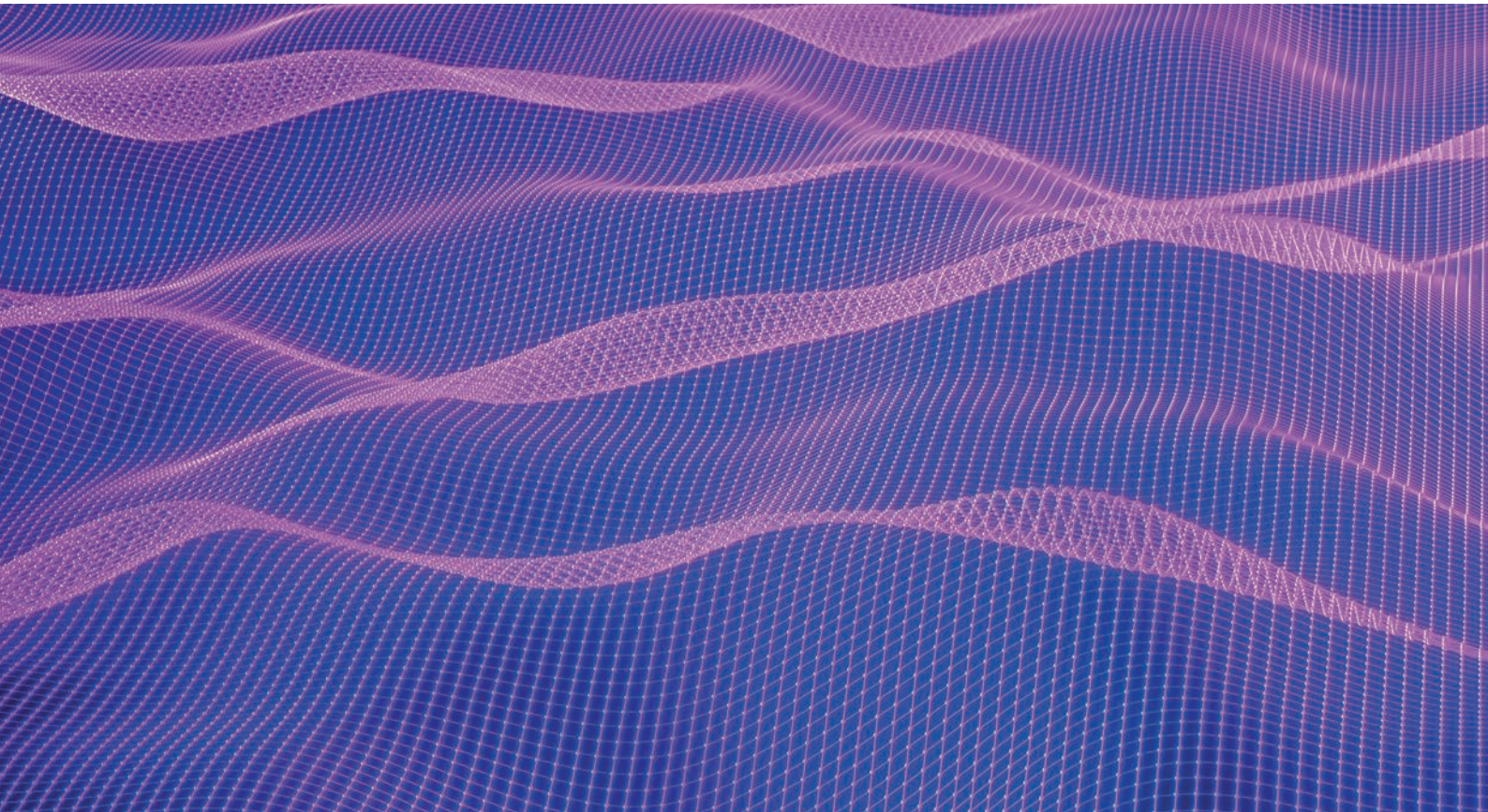
Applying this in the metaverse, the first issue to consider will be which rights apply to which individuals? As discussed above, the issue of jurisdiction is also applicable here. Today's privacy laws largely focus on the physical location of the consumer. In a physical world this makes sense. But in 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

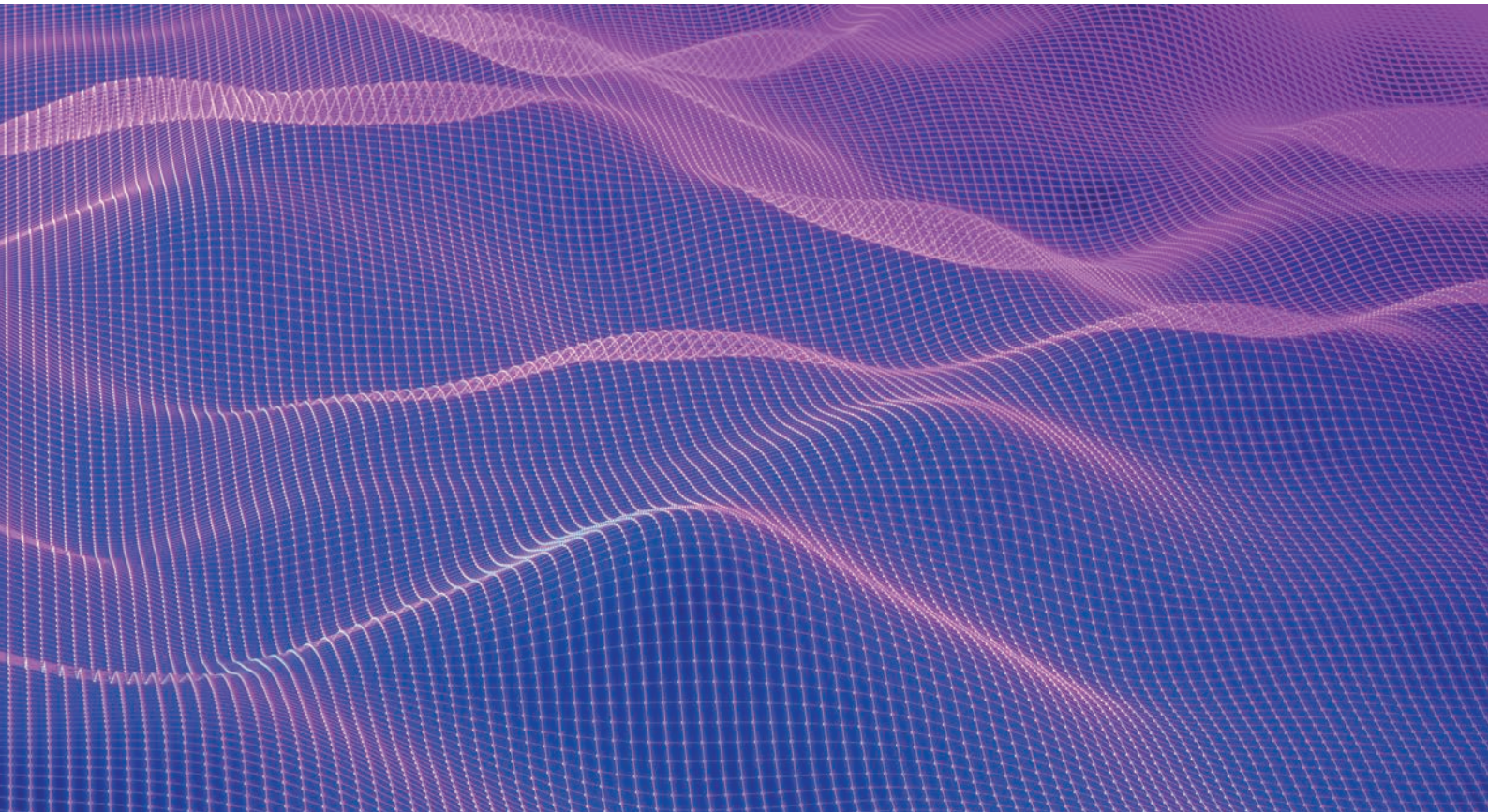
AdTech already exists in the gaming industry where providers give advertisers opportunities to place advertisements in-game, such as on billboards or jerseys and other in-game items, and the AdTech ecosystem has begun to find a way to support advertising opportunities in the metaverse. Besides the obvious 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