
“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.”

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.

Determining who is responsible and which laws apply to the metaverse will be challenging

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.

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

Most privacy laws around the world have as a central component the principle that individuals should know how their personal data is being used, by whom, and for what purposes. 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. With complex technical use cases for data on the rise, this can lead to a situation in which individuals are confronted with pages and pages of privacy notices seeking to explain how their data is used and thereby put off even attempting to read them in the first place. Imagine trying to write a privacy notice for the metaverse – let alone then keeping it up-to-date!

Then imagine that one's journey through the metaverse isn't just an engagement with one organization and controller but more akin to a trip to a mall with the possibility to seamlessly move from one store to another with advertising and offers from others along the way. How to operationalize privacy laws obsessed with transparency, tracking, and controls in such a world? With cookie pop-up mechanisms already the bane of many an Internet surfer's life, will users be confronted with pop-ups and clickwraps before their eyes 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?

The data sharing required for the metaverse to operate will be immense and 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 wholly on their profile, preferences, and actions.

Much like the AdTech ecosystem we see today, personalization of experience is often very personal-data-heavy and involves the collection, combination, and transfer of huge data sets from a number of different sources. This can include both off-line and online personal data, such as the user's grocery shopping preferences, all the way up to their inferred age, gender, and even health status, often gathered based on Internet browsing history. This provides organizations with the most accurate representation of their users. In a world where personalization is everything, this will be crucial for the metaverse and arguably even more intense than what we see online today since it will allow almost every part of an individual's life to be personalized, targeted, or advertised to in some way.

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. Again, a useful analogy here is AdTech, which relies on a network of contracts – many standard form, some bespoke. How will such a nexus of contracts – which would have to account for the sharing of personal data to and from hundreds (if not thousands) of entities – be negotiated and signed, and take account of any and all applicable governing laws?

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. There are also a number of jurisdictions with data localization requirements. How will the metaverse take into account (or not) such requirements, given its all-encompassing, global reach? Will regulators be able to provide templates and guidance to allow the right balance between efficiency, pragmatism, and protection of privacy rights for individuals?

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. Particularly in Europe, individuals are active in exercising their "right to be forgotten" and the "right to access" their personal data, and many organizations in the last few years will have dealt with requests from consumers or 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 there are a number of exemptions and exceptions, which means that individual rights will not always need to be complied with. 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 explained above, this will differ depending on which privacy rules apply. Then, operationally, how will the functionality to exercise these rights be built into the metaverse? And finally, who will be responsible for complying? Under the GDPR, it is the controller's responsibility to ensure that individuals can exercise their rights and comply with them – again, in a world where there may be many controllers, it may not be immediately apparent who is responsible for this and how the exercise of rights in one area may have implications or limits elsewhere.

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 the AdTech ecosystem will find a way to support advertising opportunities in the metaverse. Besides the obvious data and privacy issues we addressed earlier, 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, such as:

- Measurement and cross-platform tracking of ads is already an issue in the advertising industry, especially in light of the imminent demise of the use of cookies across many search engines and platforms and the ever-changing landscape of privacy laws. Advertisers should ask: How does measurement and tracking of ad performance in the metaverse work? How are standards set? Who is responsible for measuring ad performance?
- 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 online fraud the 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?

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.

Elle Todd
Partner
London
etodd@reedsmith.com

Tom Gates
Associate
London
tgates@reedsmith.com

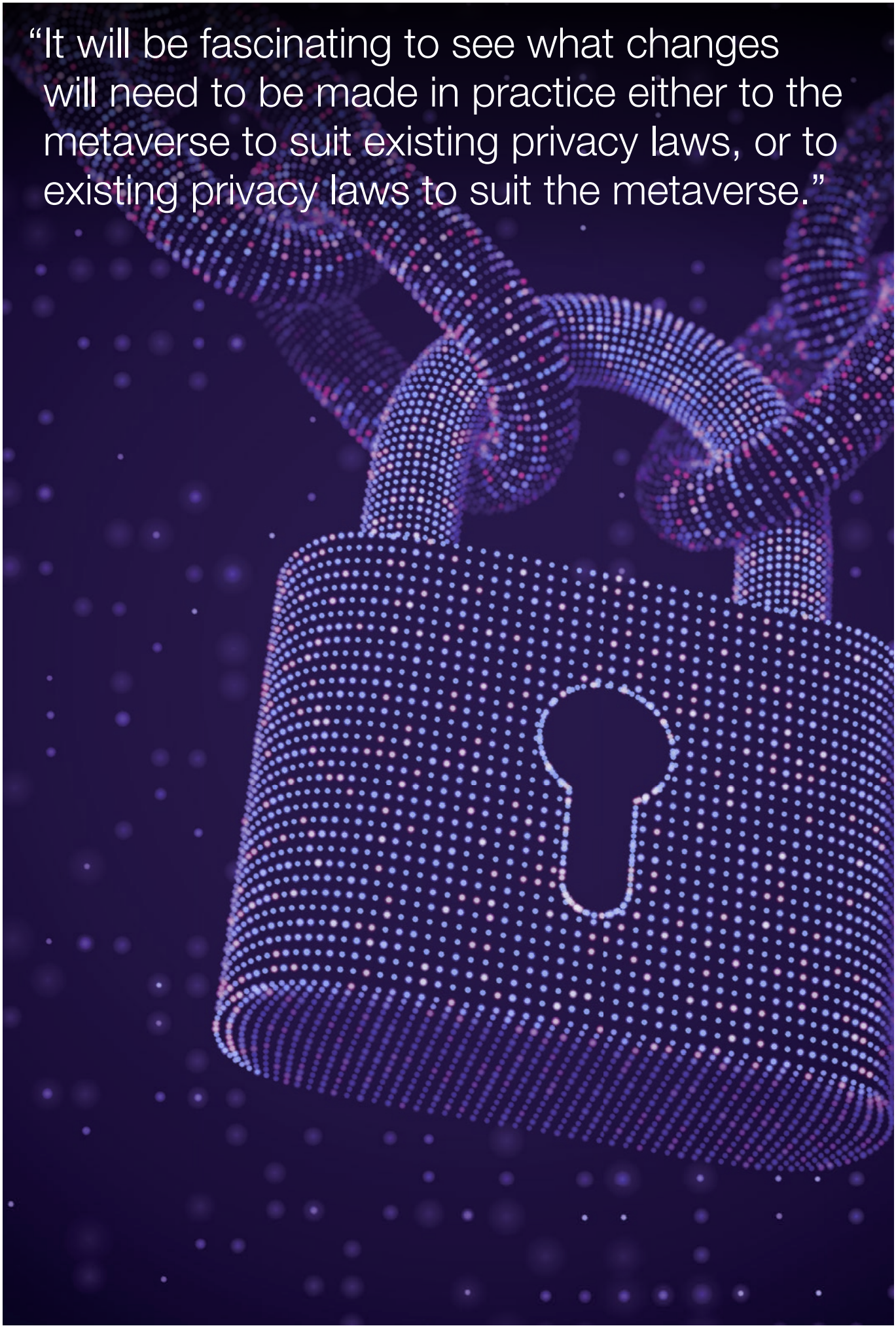
Keri Bruce
Partner
New York
kbruce@reedsmith.com

Andreas Splittgerber
Partner
Munich
asplittgerber@reedsmith.com

Hubert Zanczak
Associate
Chicago
hzanczak@reedsmith.com

Charmain Aw
Counsel
Singapore
caw@reedsmith.com

Wendell Bartnick
Partner
Houston
wbartnick@reedsmith.com


“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.”