Matheson

Ready to Enter the **Metaverse?**

What, Why and Where to Watch Out

Contents

DID YOU KNOW

An estimated 2.62 million Google searches for the term ‘metaverse’ were made in October 2021[1].

[1] MRS Digital https://europeangaming.eu/portal/latest-news/2021/11/02/103027/search-data-reveals-absolutely-no-one-understands-the-metaverse/

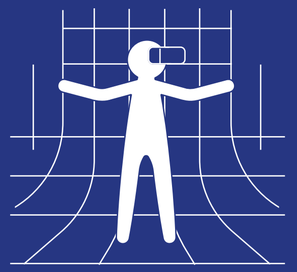
What is the Metaverse?

The term “Metaverse” has rocketed from obscurity to the top of our newsfeeds in recent weeks. Up until now, the concept has only been found in the R&D departments of big tech companies. Rapidly, the majority of these companies are launching products to the market.

The term most readily conjures up movies like *Ready Player One*, *Minority Report*, *Avatar*, *Wreck It Ralph*, *Tron*, and *The Matrix*. The likely results?

- A new way of training or storytelling, using shared gaming platforms;
- Advances in virtual / augmented / extended reality experiences;
- Enabling growth of the digital or virtual economy, non-fungible tokens and cryptocurrencies; or
- A new space in which to more freely allow for user-generated content.

At its simplest, the Metaverse represents the next iteration of the internet – a 3-dimensional version of the internet which fully immerses the user, rather than simply looking in from the outside. This will lead to an ever increasing blurring of the lines between the virtual and physical world.



“alternate digital realities where people work, play, and socialize. You can call it the metaverse, the mirror world, the AR Cloud, the Magicverse, the Spatial Internet, or Live Maps, but one thing is for certain, it’s coming and it’s a big deal.”

Forbes

How will it work?

New hardware and devices will represent the access point to this content, most likely in the wearable space. Contrastingly, the Metaverse will also incorporate the application of real-world features to the virtual world. Participants will be able to experience ever more lifelike content which has been generated for the virtual space. As visual and design technology improves, so too will a participant's feeling of immersion in a virtual environment.

WORKING LIFE
Attend meetings virtually

EXPERIENCES
Navigate lifelike "virtual" cities with your own avatar

COMMERCE
Immersive shopping experiences

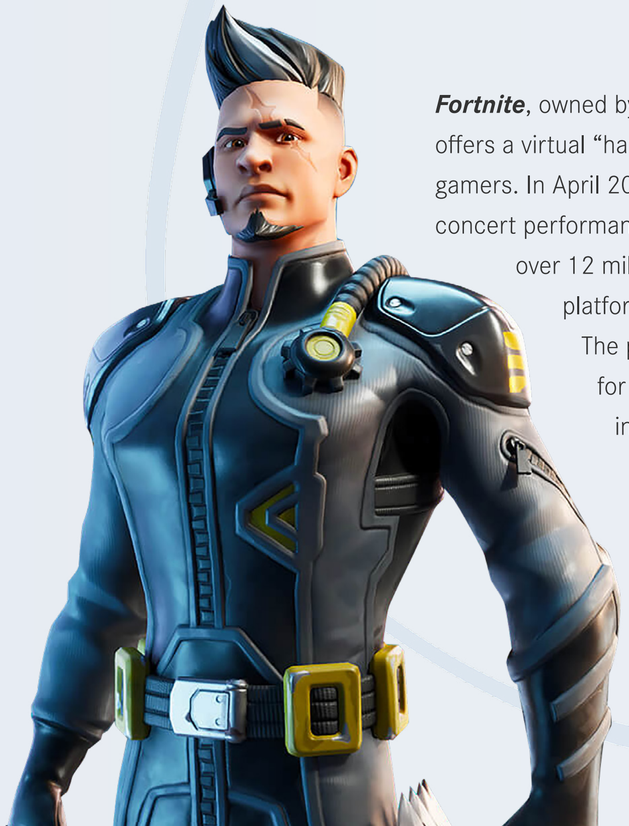
How will it work?

GAMING

The Gaming industry is spear-heading the creation of 3D worlds in which users can navigate, communicate, browse and buy products using their own avatar

Are Gaming Companies Creating "The Metaverse"?

Not quite yet. One of the key principles of the Metaverse will be a seamless degree of interoperability. Currently, the each gaming platform has its own entry requirements, without the ability to navigate between them seamlessly. The Metaverse will require the free movement of participants, goods and services on a cross-platform basis before it can be said to truly exist.



Fortnite, owned by Epic Games, now offers a virtual "hang out" space for gamers. In April 2020, a live, virtual concert performance was watched by over 12 million participants on the platform at the same time[1]. The platform is well known for its collaboration with international brands and other intellectual properties, to create in-game "skins" and digital clothes.

Roblox, a key competitor to Epic Games, recently went public under an IPO for a value in excess of $39 billion and is also making inroads into more immersive experiences. The company has partnered with car makers and fashion brands, creating virtual theme parks in which customers can interact with online simulations of their products, forging new and lasting relationships with younger consumers. These virtual products often sell well in excess of their real world value[1].

[1] The video-game industry has metaverse ambitions, too | The Economist

Why is it important?

This concept of a seamless commercial interconnectivity between proprietary virtual spaces is one of the key visions for businesses looking to engage with the Metaverse. The global technology giants are well positioned to advance and shape the future development of the Metaverse, while businesses in the financial, media and retail sectors are likely to see significant opportunities.

Increased inter-operability, greater exposure between businesses and consumers

Greater commercial reach

Potential for instantaneous purchase without browsing multiple websites or apps

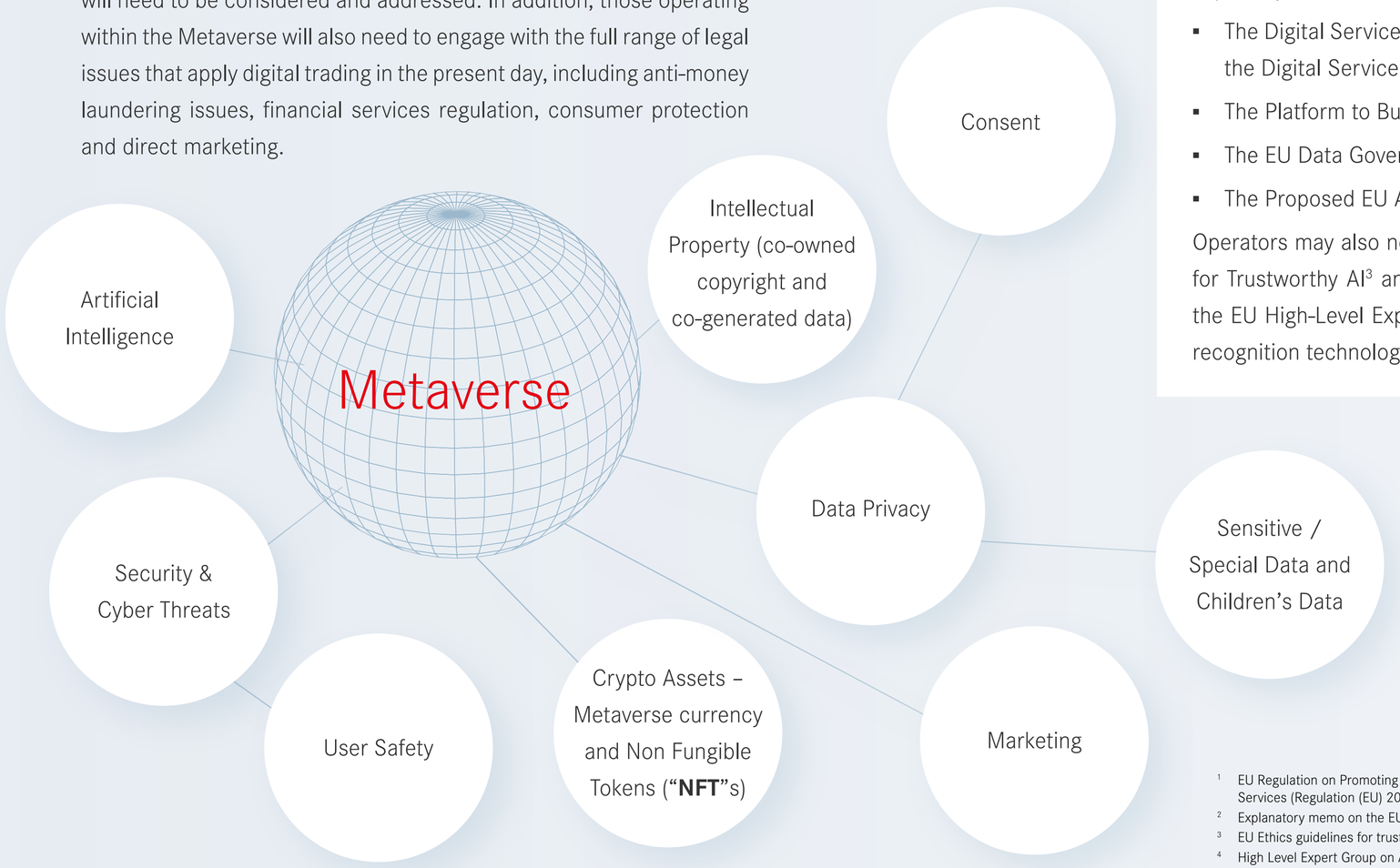
Hyper-personalised sales processes

Potential for seismic change in the way consumers work, socialise and seek entertainment

Emergence of new product and services market categories

Where are the legal challenges?

As with all new developments, the Metaverse and its associated products and services will result in a number of additional legal challenges that will need to be considered and addressed. In addition, those operating within the Metaverse will also need to engage with the full range of legal issues that apply digital trading in the present day, including anti-money laundering issues, financial services regulation, consumer protection and direct marketing.



The regulatory response to the Metaverse will be intriguing, especially in the context of:

- The Digital Services Act Package (a proposal made up of the Digital Services Act and The Digital Markets Act);
- The Platform to Business Regulation[1];
- The EU Data Governance Act[2]; and
- The Proposed EU Artificial Intelligence Regulation.

Operators may also need to consider the Ethics Guidelines for Trustworthy AI[3] and the 7 key ethical requirements[4] of the EU High-Level Expert Group, especially where emotion recognition technology and biometrics are in use.

1 EU Regulation on Promoting Fairness and Transparency for Business Users of Online Intermediation Services (Regulation (EU) 2018/0112).
2 Explanatory memo on the EU Data Governance Act
3 EU Ethics guidelines for trustworthy AI
4 High Level Expert Group on Artificial Intelligence; 7 key ethical requirements

Challenge: data privacy

User participation in the Metaverse will involve the collection of staggering amounts and types of personal data. Currently technology and cookie software allows businesses to understand how individuals navigate online sites or apps. But tomorrow, in the Metaverse, these organisations, through the kinds of advanced technology we have already mentioned, will be able to gauge a much deeper understanding of consumer behaviour through information on an individual's movements, their physiological responses and potentially even brainwave patterns. In the Metaverse, a participant's data may be gathered in the background while they go about their non-virtual lives.

Combine with this the fact that Metaverse participants are also going to be "logged in" for far greater periods of time and a situation arises whereby companies have access to data which will enable them to market in an incredibly targeted way.

It will be up to legislators and supervisory authorities, at a national and global level, to keep pace with the technological advancements in this area. As such, it is anticipated that the types of data processing which will occur in the future of the Metaverse will come with greatly enhanced data protection responsibilities. However, the nature of the Metaverse raises various questions as to how that compliance will be achieved in practice.

For example, under the GDPR entities will have varying obligations from a data protection perspective depending on whether they qualify as a data controller or a data processor.

Adding to the possibility that employers may be tasked to embrace the Metaverse as part of the workplace (e.g. immersive meetings). Employment contracts and policies will need a refresh to meet the new world of working.

Who is responsible for ensuring the security of personal data in the Metaverse? How should cross-platform participants be provided with the necessary data privacy notices? What kind of data sharing arrangements or agreements will be required between businesses? And, perhaps most crucially in the context of the increased prevalence of sensitive or 'special category' data in the Metaverse, how and when should a participant's consent be collected by companies utilising their data?

The answers to these questions may only become apparent once we see more frequent and large-scale real world examples of the types of business-to-business and business-to-consumer relationships which will come into play once the Metaverse develops beyond its current state.

In the Metaverse, establishing which entities determine how and why personal data will be processed will involve picking apart a highly complex and entangled web of relationships, to which there may be no obvious or clear answers.

Challenge: data consent and special data

As we've already mentioned, increasingly advanced hardware such as VR/AR headsets and glasses will likely be commonplace features of the Metaverse. These devices have the potential to collect a very wide range of sensitive information about the wearer, including biometric data. To the extent that this 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 Article 9 of the GDPR.

With this being the case, the user would need to give their explicit consent for each purpose for which such data is used - a general marketing consent is highly unlikely to suffice. Quite how this consent would be sought and given will be an intriguing development for businesses and legal professionals. For example, a person's sexual orientation, if disclosed to the wrong party, may result in a criminal offence, noting approx. 70 countries still criminalise same-sex relationships, with some permitting the death penalty.

Children's data is another obvious example of sensitive data requiring extra safeguards in the Metaverse. Article 8 of the GDPR will also mandate that age verification techniques, age restrictions and measures to deter children from providing their personal data are going to be essential components of data protection compliance. Added to this are the "Fundamentals for a Child-Orientated Approach to Data Processing"[1,2] recently issued by the Irish Data Protection Commission.

Aside from the data safeguards, experts are also considering the effects of VR on children being very different to holding a device in one's hands. Parents and carers will be seeking ways to protect their children's privacy, health and wellbeing, and especially protect against malicious threat actors.

A question of consent?

As people move through the Metaverse, how will their personal data be managed? Consent as a key principle under GDPR which will demand greater focus by all legal professionals, supervisory authorities and data controllers alike. Consent is linked with privacy being a fundamental human right. Questions may arise around which rules govern the consent (and also purpose, retention etc), given that we could be looking at multiple countries and local laws. The intent is for the Metaverse to be global and not chained to a single platform. However, this will need to be carefully tested in the context of varying GDPR compliance across Europe (e.g. United Kingdom following its departure from the EU), the USA (Privacy Shield / Schrems II), and further afield.

1 Data Protection Commission "Fundamentals for a Child-Orientated Approach to Data Processing"

2 Data Protection Commission, "Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing": Report on Public Consultation, November 2021

Challenge: intellectual property

The application of existing principles of joint authorship and co-ownership are likely to come into focus in virtual world scenarios where there is a whole community of IP stakeholders involved. It is for this reason that the European Commission is considering legal reforms to clarify the position on "co-generated" data arising out of new tech. This was mentioned in a strategy report published by the European Commission in 2020[1].

From a licensing perspective, the fast-moving world of the Metaverse will involve concepts such as (from a gaming perspective, for example) character "mash-ups" and more generally the bringing together of co-owned IP rights. Another element is that, given the scale of content creation envisaged in the Metaverse, interaction between traditional IP owners (i.e. brands) and user-generated content will become not only common, but essential to its development and attractiveness. Brands are going to have to consider their approach to protecting and enforcing their IP when it interacts with this user-generated content. This issue is not unknown to professionals, e.g. YouTube content creators. It is the ability to identify these developments across a complex environment is a key challenge.

With this in mind, any brand seeking to interact or experiment in the Metaverse should immediately look to establish IP licensing arrangements with the relevant platform providers, with special attention paid to the scope of such licences.

In this regard, trademark owners will have to be particularly aware of certain issues. For example, a brand which invests in creating virtual content on one platform and which then wishes to use this content in a different context (i.e. by transferring or 'porting' it into a separate platform or experience), should seek to ensure that its contract with the Metaverse vendor grants all the necessary IP rights to give the brand flexibility on future use.

On the other hand, however, a brand might wish to veto the use of its virtual content in the context of certain platforms or experiences, and setting out the limits of use at the outset will help to avoid disputes down the line. The steps a partner platform can take to remove or censor infringing content should also be clarified through the appropriate terms of use.

Copyright and the Metaverse: benefits and risks

From a copyright perspective, the Metaverse presents some potential benefits. For example, developers could leverage being the first to develop particular area of the Metaverse to obtain royalties for the use of copyrighted software. However, it may also create risks. Policing the Metaverse for piracy of copyrighted works is going to be highly challenging. Additionally, content creators who may be relying on existing licenses to create digital content for the Metaverse should seek to ensure that those licenses cover the use of the copyrighted work, not only in its existing format, but also within the Metaverse.

[1] The European Parliament "Regulating facial recognition in the EU": https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf

Challenge: use of crypto-assets

In order for the Metaverse to truly realise the commercial potential being presented by technology companies and the gaming industry there will need to be an instant, secure, transparent and traceable method for businesses to conduct transactions with one another and with their consumer base. In this regard, crypto assets and blockchain technology may provide an answer.

Many platforms are already running on blockchain technology and are using crypto assets, such as Non-Fungible Tokens ("**NFT**"s), to construct, own and monetise unique decentralised assets. Blockchain offers a secure, immutable and decentralised database which enables countless virtual sources to interact in one common network. Within this, crypto assets and tokens provide a means of carrying data securely, allowing companies and individuals to transfer virtual content, personal data and other encrypted information.

Examples of NFTs are found in virtual games, *Fortnite* and *Roblox*, where brands seek to reach consumers via these types of games, from designing limited edition "skins" or collections for their avatars, to giving access to exclusive events. In November 2021, Vogue Business held a summit with Google with executives from Burberry, Roblox, and other consumer brands to discuss the Metaverse and NFTs ("The Technology Fuelling Fashion's Next Phase")[3].

Any trading in digital currencies will need assessment from a financial regulatory perspective. For example, would it qualify as a security?

If using NFTs, is the a party aware that ownership does not necessarily transfer automatically and may need to be formally documented. After all, an NFT is software code that verifies ownership only. On the plus side, they are interoperable and have the potential to be traded outside of their original environments and in any currency.

"an online arena where "decentralized finance," or DeFi, reigns – fusing together cryptocurrencies, blockchain technology, non-fungible tokens and video gaming."
Bloomberg[2]

[1] The European data strategy: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy
[2] https://www.bloomberg.com/news/features/2021-10-30/what-is-the-metaverse-where-crypto-nft-capitalism-collide-in-games-like-axie
[3] https://www.voguebusiness.com/technology/personalisation-the-metaverse-and-nfts-the-technology-fueling-fashions-next-phase

Challenge: use of artificial intelligence

Artificial intelligence and machine learning will be key to the development of the Metaverse. The legal question is whether the EU will consider the Metaverse as part of the debate around the new draft EU Artificial Intelligence Regulations.

As mentioned in the context of data privacy, biometric data may be disclosed through the use of the Metaverse (e.g. via the wearable technology). The European Parliament noted that Artificial intelligence ("**AI**") powers the use of biometric technologies, including facial recognition applications, which are used for verification, identification and categorisation purposes by private or public actors[1].

While facial recognition markets are poised to grow substantially in the coming years, the increasing use of facial recognition technologies ("**FRT**"s) has emerged as a salient issue in the worldwide public debate on biometric surveillance. While there are real benefits to using facial recognition systems, they give rise to a number of fundamental rights concerns with regard, for instance, to discrimination against certain segments of the population and violations of the right to data protection and privacy.

The European Parliament has pointed to the Charter of Fundamental Rights, the General Data Protection Regulation, the Law Enforcement Directive and the EU framework on non-discrimination, which also apply to FRT-related processes and activities. The draft EU AI Regulation is intended to restrict use of biometric identification systems that could lead to ubiquitous surveillance.

The technology to be used in the Metaverse will also need to consider the various tests set out in the draft EU AI Regulation, such as conformity assessments, determining "high-risk" or "low-risk" characteristics, and where the questions around biometrics finally land. Ultimately, the question of trust will need to be solved by the creators.

[1] The European Parliament "Regulating facial recognition in the EU": https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf

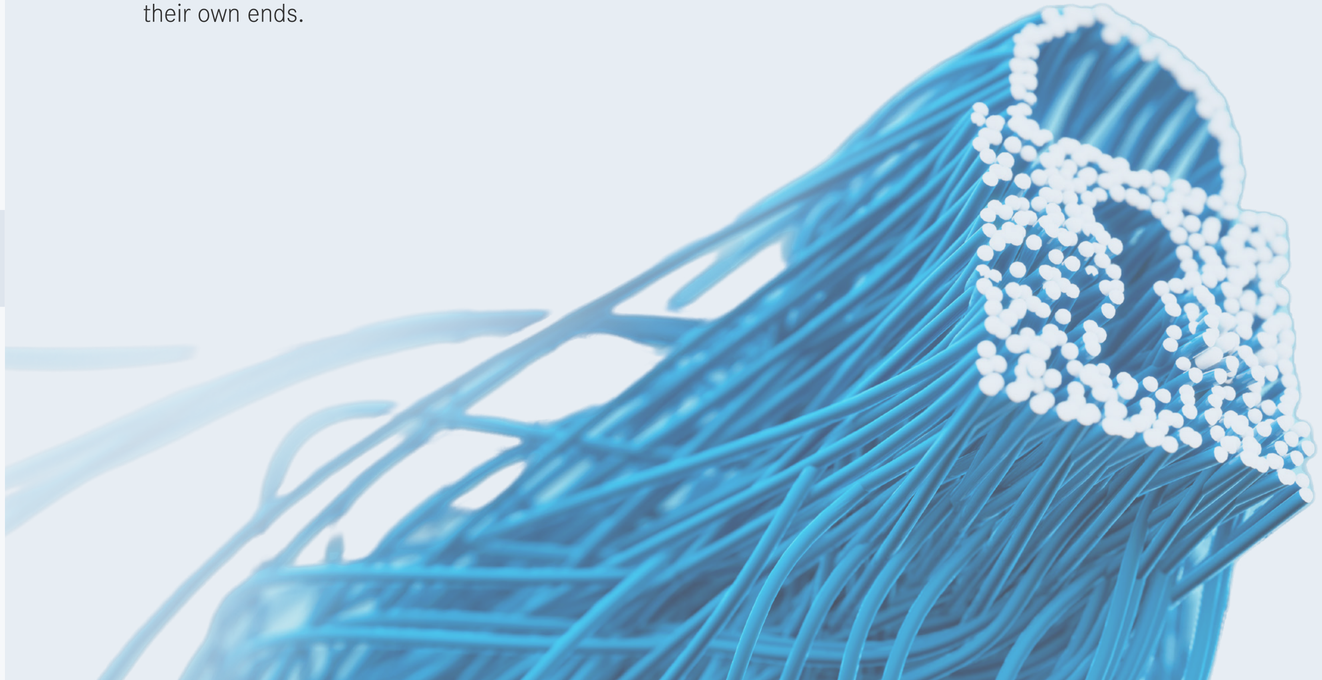
Challenge: security and cyber threats

As the Metaverse expands its offerings as a marketplace for both commerce and personal data, more and more consumers will shift their digital lives from the current computer and mobile internet model to the Metaverse.

As with any current underlying legacy system, this increase in traffic raises the risk and attractiveness for a potential cyber attack. For example, research into a number of popular Virtual Reality ("**VR**") platforms previously found that there was little in the way of protection at the time for VR being hosted on a compromised computer. Hackers faced little in the way of encrypted software and were able to interfere with a platforms proprietary content to alter a user's VR experience to their own ends.

Elements such as integrated contactless payment systems, the increased prevalence and storage of biometric data and massive amounts of cross-platform data transfers will all increase the risk profile for consumers and businesses in the Metaverse. Enhanced, and perhaps yet uninvented, security frameworks will be required to protect against malware attacks, fraud and data breaches.

Simultaneously, new and updated legislation will be required to address the enhanced security risks presented by the Metaverse. While business players wait for this they may want to follow a predicative rather than reactive approach to regulation.



Challenge: user safety

Concerns will only increase over the impact which harmful or malicious content could have on participants in the Metaverse. The all-encompassing sensory experience which will, via virtual and augmented reality, integrate the Metaverse into a user's daily life will likely exacerbate the psychological effects of such content.

Companies operating digital platforms in the Metaverse will need to find ways in which to mitigate these risks, a monumental task given the context of potentially billions of real-time interactions.

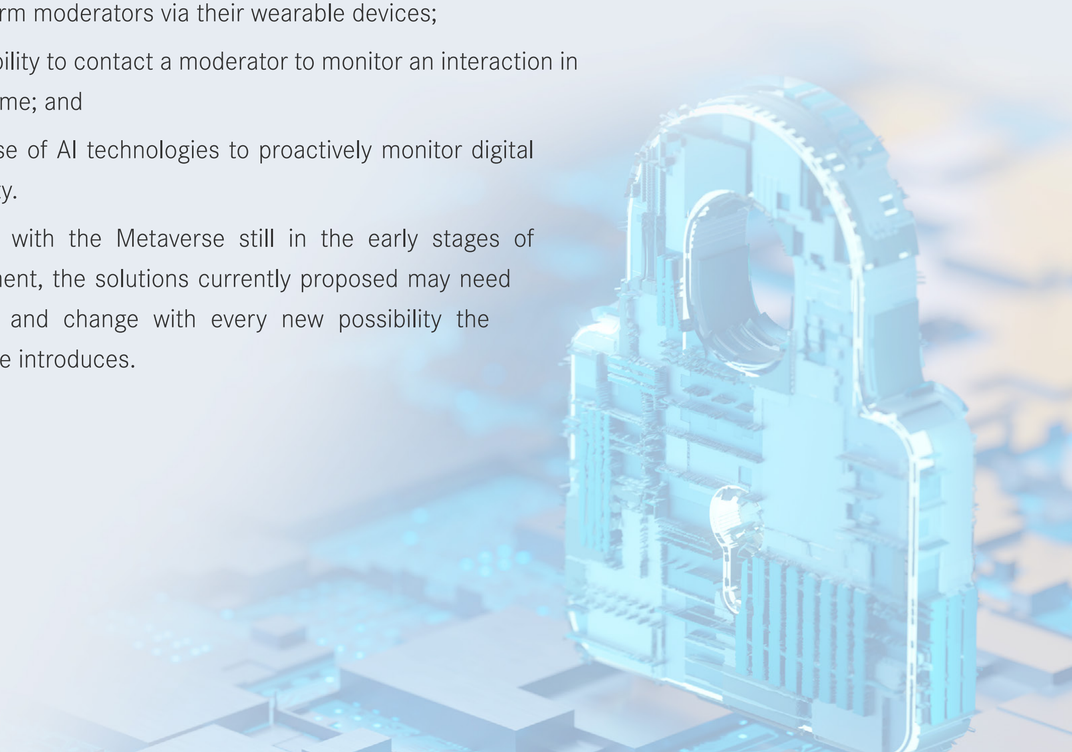
Traditional methods of moderating online platforms may not be suited or effective when it comes to the Metaverse. Extensive review processes carried out on new developers or content would significantly hinder the stated aim of a space in which users can freely generate and share their own content. Similarly, companies must now consider how to update their moderation processes to include content which does not fall within the traditional categories of images, videos or messages – in the Metaverse, moderators will have to contend with 3D, real-time avatars, meaning that actions, behaviours, movements and gestures will all come into play. Traditional sanctions may also fail dissuade bad behaviour in the Metaverse. If the envisaged level of interoperability is achieved, then a suspension or ban from one platform may not necessarily prevent the offending party from simply taking their digital avatar / content and migrating to another.

Companies and developers may need to consider parallel enforcement for sanctions imposed on offending parties in the Metaverse. As much as cross-platform cooperation will be required to encourage and build the Metaverse, it will also be crucial to maintaining it as a safe place for users.

Some of the larger technology players have already begun the process of exploring solutions to these emerging user safety risks. Suggestions to date have included:

- providing users with the tools to record and report bad behaviour to platform moderators via their wearable devices;
- the ability to contact a moderator to monitor an interaction in real-time; and
- the use of AI technologies to proactively monitor digital activity.

However, with the Metaverse still in the early stages of development, the solutions currently proposed may need to adapt and change with every new possibility the Metaverse introduces.



Key contacts

“Are you ready, Player One?”

Matheson’s highly experienced Technology and Innovation Group will be keeping abreast of developments in this area as it progresses.
At this stage, we would be very interested to hear from you on your expectations or questions about these developments.

Anne-Marie Bohan
Partner | Head of Technology and Innovation
E: Anne-marie.bohan@matheson.com
T: +353 1 232 2212

Rory O’Keeffe
Partner | Technology and Innovation
E: rory.o’keeffe@matheson.com
T: +44 7732 901 893

Deirdre Crowley
Partner | Technology and Innovation
E: deirdre.crowley@matheson.com
T: +353 1 232 3710

Carlo Salizzo
Senior Associate | Technology and Innovation
E: carlo.salizzo@matheson.com
T: +353 1 232 2011

Questions, Suggestions, Feedback?
Let us know here!

Report authors

Rory O'Keeffe
Partner | Technology and Innovation
E: rory.o'keeffe@matheson.com

Edmond James
Trainee Solicitor | Technology and Innovation
E: edmond.james@matheson.com

DUBLIN
70 Sir John Rogerson's Quay,
Dublin 2
Ireland

T: +353 1 232 2000
E: dublin@matheson.com

CORK
Penrose One,
Penrose Dock, Cork,
T23 KW81

T: +353 21 465 8200
E: cork@matheson.com

LONDON
1 Love Lane
London EC2N 7JN
England

T: +44 20 7614 5670
E: london@matheson.com

NEW YORK
200 Park Avenue
New York, NY 10166
United States

T: +1 646 354 6582
E: newyork@matheson.com

PALO ALTO
530 Lytton Avenue
Palo Alto, CA 94301
United States

T: +1 650 617 3351
E: paloalto@matheson.com

SAN FRANCISCO
156 2nd Street
San Francisco CA 94105 United States

T: +1 650 617 3351
E: sf@matheson.com

Matheson