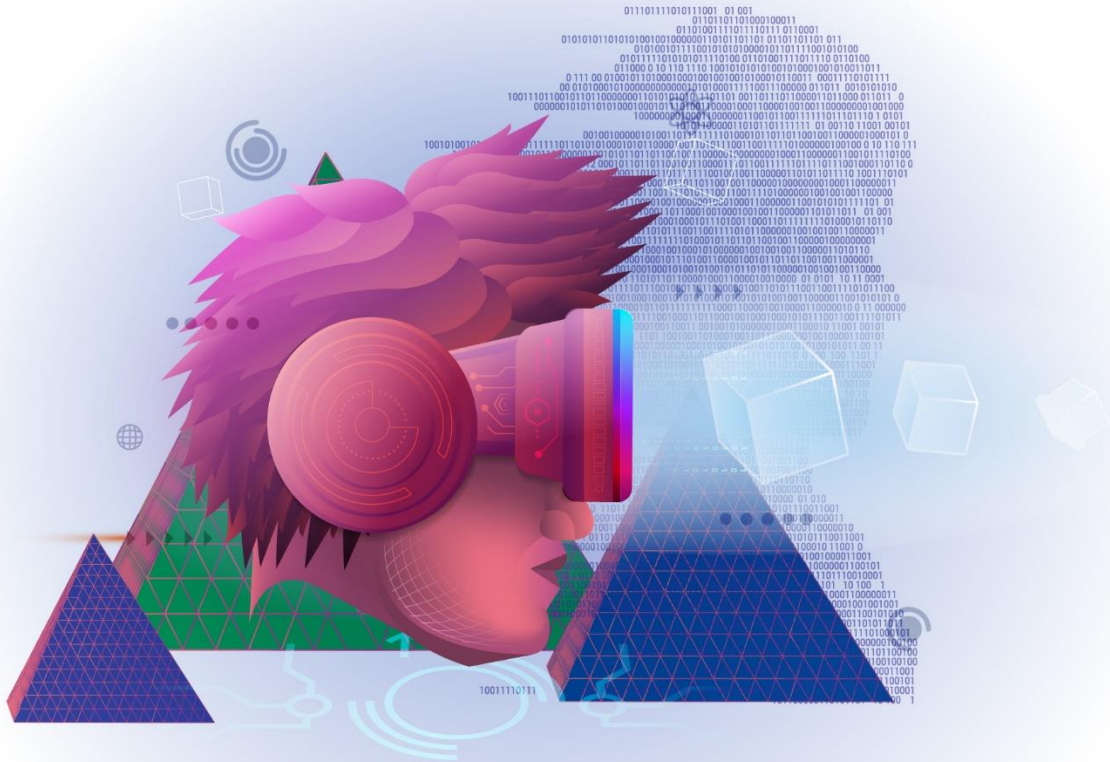


RAJAH & TANN ASIA

LAWYERS  
WHO  
KNOW  
ASIA

DATA & DIGITAL  
ECONOMY:  
BEYOND THE HYPE  
OF THE METAVERSE



RAJAH & TANN ASIA

CAMBODIA | CHINA | INDONESIA | LAOS | MALAYSIA | MYANMAR | PHILIPPINES | SINGAPORE | THAILAND | VIETNAM

[www.rajahtannasia.com](http://www.rajahtannasia.com)

# CONTENTS

|  |    |
|--|----|
| Introduction                                 | 3  |
| Digitalisation and the “Metaverse”           | 5  |
| Media  | 7  |
| Intangible Assets & Rights Management        | 10 |
| Finance and Payments                         | 13 |
| Infrastructure and Sustainability            | 15 |
| Real Estate                                  | 18 |
| Retail and Commerce in the Metaverse         | 20 |
| Privacy, Data Protection and Data Governance | 23 |
| Cybersecurity and Cybercrimes                | 25 |
| Ethics                                       | 31 |
| Dispute Resolution                           | 29 |
| Our Achievements                             | 31 |
| Our Regional Contacts                        | 34 |
| Disclaimer                                   | 42 |

# Introduction

It is often said that the only constant in life is change, and one need look no further than the screen in front of them for an undeniable example of this. Whether it be a computer, a phone, or any other device, the 'next generation' comes along at shorter intervals, while the scope of the user experience widens with longer strides. As technology continues to advance at unimaginable speeds, changing the way we live, work and play, we must look towards the ever-approaching horizon and ask ourselves: what's next?

The latest feature in the line-up of 'next-big-things' has been the advent of the metaverse, which has promised to revolutionise lifestyle, commerce, and business. But as the hype cycle runs its course, and the industry begins to question the actual impact of the metaverse, it becomes increasingly important to look beyond the superficial and towards what the metaverse truly represents – the continued and exponential digitalisation of the world around us. From that vantage point, we can strip back the buzz and begin to see the real legal issues at play, which all revolve around the common axis of Data and Digital Economy.

With the incremental advancement of the Data and Digital Economy space, individuals and businesses will be faced with both opportunities and challenges. The commercial and investment opportunities associated with digitalisation and the metaverse are vast, and businesses would be well advised to begin preparatory steps towards capitalising on such prospects.

However, this may be easier said than done. The developmental and exploratory nature of Data and Digital Economy means that there will be uncertainties abound regarding how to operate in this unfamiliar space. In particular, users and businesses will have to grapple with complex legal issues spanning numerous areas of law – issues that will require multi-disciplinary expertise to effectively navigate.

In this article, we take a closer look at Data and Digital Economy and the concept of the metaverse, the various sectors to explore opportunities that may arise, as well as the respective legal issues that will undoubtedly be intertwined with such opportunities. The main sectors we have considered are:

- Content
- Intellectual property & tangible rights and assets
- Finance and payments
- Infrastructure and sustainability
- Real estate
- Retail and commerce
- Privacy, data protection and data governance
- Cybersecurity and cybercrime
- Ethics
- Dispute resolution

The issues raised in our progress towards Data and Digital Economy traverse a wide scope of sectors and disciplines, are not confined by jurisdictional boundaries, and cannot be managed in isolation. To fully address the various challenges of organisations seeking to stake a claim or have a presence in this sphere, Rajah & Tann offers a full suite of Data and Digital Economy services.

Rajah & Tann Asia is a network of law firms with expertise across Corporate and Dispute services, and is closely supported in the areas of LegalTech and cybersecurity by network members Rajah & Tann Technologies and Rajah & Tann Cybersecurity. By merging core Data and Digital Economy skillsets with the various specialist practices across the Rajah & Tann network, we draw on the strengths and expertise of each lawyer to provide clients with multi-disciplinary, multi-legal, and transnational solutions.

Our Data and Digital Economy group covers the gamut of practices that make up the metaverse, and includes the following:

- Artificial Intelligence & Data Analytics
- Cloud, Data Centre & Info-Communications
- Cybersecurity & Cybercrime
- DDE Disputes & Crisis Management
- DDE Mergers & Acquisitions
- Digital Media, Social Media & Online Falsehoods
- Electronic Commerce, Trade & Consumer Protection
- Fintech, Blockchain & Smart Contracts
- Intangible Assets, Intellectual Property & Media
- Privacy, Data Protection & Data Governance

The information in this guide is accurate as of May 2023.

## Digitalisation and the "Metaverse"

*Before delving into the prospective sectors, we need to know what the hype is about. To give a better understanding of the ground we will be traversing, we answer some of the most commonly asked questions: What does Data and Digital Economy entail? Where are we on the route of digitalisation? And of course, what exactly is the metaverse?*



People often speak of the digital world as a foreign or future location. In reality, the digital world is not too distinct from the real world, and the boundaries are quickly dissipating. Financial services are shifting to the digital sphere, working from home is becoming the norm, and our interactions take place far more often online than in person. After all, what is the real world but the world we live in?

This is why the concept of Data and Digital Economy goes beyond issues of technology. It covers the digitalisation of trade, whether in physical goods or digital assets; it covers the continually growing digital economy; it covers the sovereignty and protection of data, which underpins the conduct of transactions and commerce.

The continued digitalisation of our world is undeniable. What then is the metaverse's role in this process, and what is the metaverse in actuality? Just as how the technology of today would have been difficult to imagine from the viewpoint of an earlier generation, the eventual




form that the metaverse will take is, of course, difficult to predict. What we do know is that the general concept of the metaverse exists as a shared virtual environment of interconnected communities, incorporating the real-world experiences of work, leisure and commerce.

Such a reality may not be too far from fruition. The metaverse will certainly develop incrementally over the long term, but its foundations (both physical and virtual) are already being built up. In fact, one could look at Second Life, widely regarded as a precursor to the metaverse, which was introduced as early as 2003. Second Life is an online multimedia platform which allows users to create an avatar as a 'second life' on the platform, including socialising, building, shopping and trading. The platform even had its own virtual currency.

Many of these activities are already conducted online. What the metaverse represents is a natural progression of this movement, and envisions the eventual ability to conduct all these aspects of life digitally and virtually.



Perhaps we can dare to imagine ourselves similarly in the digital world, navigating the virtual reality through our self-defined avatars. From working in remote offices, to stepping into a department store to do shopping, meeting up with friends at a virtual coffeeshop, or adventuring in a game universe. At the end of the day, we return to our virtual homes to log off for the day.





|   |  |
|---|--|
|  <p><b>Work</b></p> <ul style="list-style-type: none"> <li>• Remote working arrangements</li> <li>• Virtual offices</li> </ul>   |  <p><b>Leisure</b></p> <ul style="list-style-type: none"> <li>• Social interaction on virtual platforms</li> <li>• Consumption of entertainment online</li> </ul> |
|  <p><b>Commerce</b></p> <ul style="list-style-type: none"> <li>• Virtual retail stores for physical or digital products</li> <li>• Provision of services online</li> </ul> |  <p><b>Finance</b></p> <ul style="list-style-type: none"> <li>• Online payments</li> <li>• Virtual currencies</li> <li>• Paperless transactions</li> </ul>        |

Even now, various elements of the metaverse are already in operation, such as cryptocurrencies and Non-Fungible Tokens ("NFTs"), which are continually gaining traction. The gaming industry also stands as a first mover in this area, bringing the user experience online and employing the use of augmented and virtual reality technology in new and expanding ways.

Above and beyond the various industries delving into the digital economy, one of the concepts one should consider is that the digital world is not a single discrete universe. It comprises a multitude of dimensions, each with its own services and functions, be it in retail, finance, real estate, gaming or lifestyle. Just as how the cryptocurrency world started on distinct blockchains, different platforms and wallets allow the integration of the product derived from these blockchains such as Bitcoin or Ether. The same applies to the gaming world for games with a common developer, such as Microsoft and Sony – individual games have their own avatars, but single accounts represented by a customisable single

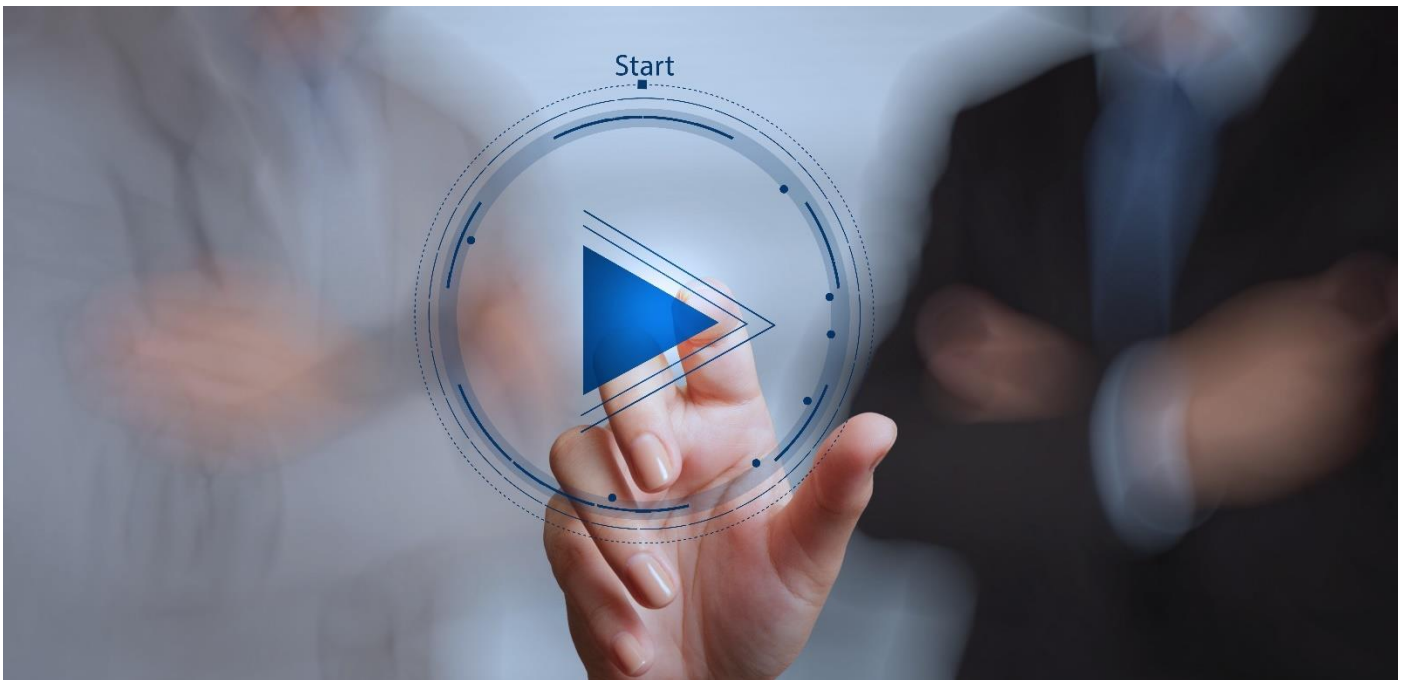
avatar are created to represent a user for all their games, allowing users to chalk up achievements across different games. In the gaming and social media world, gamers and streamers are often known by their streaming "handles" or their avatar, a concept that may well become commonplace: your digital ID.

For businesses, the remaining question is what role they will play in the metaverse – leader, follower or none at all. In order to play a leading role, businesses must tackle the legal issues associated with participating in the digital economy. As the digital economy is defined by its innovative and novel nature, the legal issues arising from such opportunities are similarly novel and unexplored. Here, we begin the necessary process of exploration by looking at the key sectors, as well as the various legal issues that may arise within each sector, including the following:

|   |  |
|---|--|
|  <p>Intellectual Property</p>         |  <p>Commercial Law</p>              |
|  <p>Regulatory Controls</p>           |  <p>Dispute Resolution</p>          |
|  <p>LegalTech</p>                     |  <p>Competition &amp; Antitrust</p> |
|  <p>Data Protection &amp; Privacy</p> |  <p>Banking &amp; Finance</p>       |

## Media

*Our progress into the digital world entails many functions and serves multiple purposes for any given user. The consumption and creation of content is expected to be one of the key foundations of the user experience. The concept of "new media" is set to evolve significantly in the metaverse and beyond, offering a new era of media consumption and creation that goes beyond traditional forms of content.*



The digital world will provide new avenues for the creation of content and media. From a commercial viewpoint, this creates new opportunities relating to the exploitation of content. The key industries involved would be the advertising, gaming, music, social media, and film and television spaces.

User generated content ("**UGC**") has become an integral part of the online experience, and its impact is expected to be far more pronounced the further we proceed into the digital experience, such as in the metaverse, where users are not just passive consumers of content but active participants who can create their own experiences and contribute to the world's development. UGC allows users to express their creativity and individuality, bringing a unique and diverse set of perspectives.

For creators, this advancement is likely to provide unprecedented access to consumers and a wider audience than previously available. New tools that are being developed with the help of new and cutting-edge

technology such as artificial intelligence can also serve to enhance the overall experience of UGC by consumers of such content, while the associated opportunities for content creators would include licensing, advertising and sponsorship.

More recently, we also see the advent of online social platforms and collaboration spaces that incorporate the use of UGC. For example, on the app Bondee, UGC is an important aspect of this experience, allowing users to create and customise their own virtual avatar and home space, and subsequently connect with other users on the app. UGC is not just a feature, but an integral part of the platform's identity and vision for the future of the metaverse.

As technologies such as UGC creates an increasingly immersive experience for users by empowering them to take an active role in shaping their user experience and facilitating seamless online social interactions, the line between reality and the virtual world is likely to become

increasingly blurred as individuals migrate a substantial portion of their lives onto digital platforms.

As with all things new, the provision of such new opportunities and avenues is likely to come with its own set of challenges. Here, we examine some of the legal issues relating to media and content in the digital world.



### Providers

Existing device and service providers may find themselves in a position where they will have to transition their services to fit the virtual world. There will also be market space for new providers to capitalise on the changing needs of users.



### Creators

For creators, the virtual world is likely to provide unprecedented access to consumers and a wider audience than previously available. The associated opportunities for content creators would include licensing, advertising and sponsorship.

## Mis-information

With the advent of social media and other enablers of UGC, the power to control media, content and online narratives is increasingly shifting to the hands of the masses, whereas in the past traditional media outlets held a monopoly over the dissemination and control of information. This increasingly diverse and decentralised media landscape has brought to the forefront a new wave of mis-information, dis-information, and even mal-information that highlights the importance of laws aimed to curb defamatory content, online falsehoods and even harassment.

- In Singapore, both traditional and alternative media sites have not been immune from sanction under the Protection from Online Falsehoods and Manipulation Act 2019 ("**POFMA**"), an act enacted to "prevent the

electronic communication in Singapore of false statements of fact, to suppress support for and counteract the effects of such communication, to safeguard against the use of online accounts for such communication and for information manipulation, to enable measures to be taken to enhance transparency of online political advertisements, and for related matters". Private parties are also provided an avenue to seek civil recourse for falsehoods propagated against them under Singapore's Protection from Harassment Act 2014 ("**POHA**").

- Doxxing is also of a growing concern in the digital age, as the ease of access to personal information on the internet and its speed of proliferation over the metaverse can lead to individuals being targeted and harassed online. The POHA is an important piece of legislation to guard against and criminally sanction users who engage in such behaviour. Online influencers, even well-intentioned ones, have not attained immunity from this and we have witnessed them both perpetuating and falling victim to such acts.

## Content Regulation

Internet content providers ("**ICPs**") and internet service providers ("**ISPs**") will also have to be aware of their compliance obligations in the various jurisdictions in which they provide content and/or services in.

In Singapore, this would include complying with the Broadcasting Act ("**BA**") and any relevant subsidiary legislation and/or code of practice issued pursuant to the BA. With the rise of platforms such as OnlyFans which allow users to create and share explicit content with little to no oversight, we may expect to see a rise in oversight by regulators of the online space in a bid to protect vulnerable individuals such as minors from media and content that is objectionable and harmful.

Singapore has also seen the recent enactment of the Online Safety (Miscellaneous Amendments) Act ("**OSA**") on 1 February 2023, which introduced a new Part 10A into the BA to regulate Online Communication Services ("**OCS**") accessible by Singapore users. This was done as part of a concerted effort to enhance and improve internet safety in Singapore. As a start, only Social Media Services ("**SMS**") have been specified and subject to provisions under part 10A.



- Part 10A enables the Info-communications Media Development Authority ("**IMDA**") to issue directions to OCS providers to disable access to egregious content by Singapore end-users and stop the egregious content from being transmitted to Singapore end-users via other channels or accounts. Such egregious content includes content advocating or instructing on suicide or self-harm, physical or sexual violence and terrorism; content depicting child sexual exploitation; content posing public health risks in Singapore; and content likely to cause racial and religious disharmony in Singapore.
- To better protect the vulnerable, a new Code of Practice for Online Safety in Singapore will also require designated SMS with high reach or high risk to have system wide processes to enhance online safety for all users, with additional safeguards for young users under 18 years of age. Users should also have access to reporting mechanisms to flag matters such as the non-consensual distribution of intimate videos.

## Regulatory Controls

The issue of jurisdiction comes into focus when one considers the regulation of media and content itself. Media and content in the metaverse would still be subject to legislation on censorship and standards. The familiar question arises as to which country's laws are applicable, particularly as the standards across different jurisdictions can have vast variations and potentially serious penalties. Parties involved in the creation or distribution of content would thus have to ascertain the applicable standards so as to ensure that they do not inadvertently breach any relevant regulations.

## IPRs

The issue of ownership and exploitation of IPRs will also be a significant issue that arises in the course of the creation, consumption and exploitation of content, which we discuss in greater detail in the next segment.

# Intangible Assets & Rights Management

*Intangible assets ("IA") refers to any asset lacking a physical substance. These range from your traditional categories of IA such as goodwill and intellectual property ("IP") (i.e., copyright, trademarks and patents), to newer forms of emerging IA such as digital tokens, cryptocurrencies and more. Questions arise not just with respect to the legal ownership of IA, but also with their protection, securitisation and exploitation.*



Given that IA can have significant real-world value, a preliminary question is when IA rights arise in the first place and who owns these rights. This enquiry is further complicated by the proliferation of UGC, as well as AI-generated content.

Further down the line, holders of IA rights wishing to exploit such rights will be looking to navigate distribution channels and to establish adequate protection over their rights to ensure that they are fairly remunerated. IA owners could face particular challenges arising from the difficulty of policing for IA rights breaches in the digital world, including the metaverse, particularly in relation to copyright.

IA rights licensees will also be looking to arrange for sufficiently broad licences. The challenge in this regard arises from the constantly evolving use cases of content in the digital world. Due to the lack of foreseeability of

such cases, it may be difficult to structure arrangements capable of sufficient adaptability.

Other issues to be considered by rights holders and users would include:

- **Agreements for distribution:** The scope of any agreement for distribution of third-party material and whether there are proper licenses to copyrighted works and other relevant IA rights.
- **Agreements with customers:** Agreements with customers and whether they protect against unintended distribution.
- **Protection of IP:** What technological measures can be implemented to protect against unauthorised distribution, and the enforcement of rights through IP litigation (of which metaverse-related litigation has been on the increase). Dealing with intangible assets in an intangible world raises questions on how

intellectual property rights can be asserted and enforced.

Businesses and organisations must be prudent in strategising new ways to commercialise their IA rights as the Data and Digital Economy is primed to provide an even larger platform for the exploitation of both new and existing rights.

**Jurisdictional issues:** When it comes to IA, apart from contractual arrangements, IA rights are also subject to the relevant IA legislation. As the digital world is not jurisdictionally-bound, the question arises as to which country's laws are applicable to a particular IA and, more fundamentally, whether the laws are able to cope with the changing dynamics in the first place. Governments may, in due course, have to establish new legislative models and IA registration and protection systems.

The issue of jurisdiction also comes into play when considering which country has jurisdiction in an action over the breach of IA rights. What if IA rights granted by jurisdiction A are breached in jurisdiction B, which is fairly likely given the nature of the digital world? Do the courts of jurisdiction A or jurisdiction B have jurisdiction over the dispute? It is important to note the trends in the approach of courts towards subject matter jurisdiction, particularly as the approaches adopted may differ from country to country.

## Brand Identity

Brand protection would be essential as users challenge the boundaries of IA rights as we know it.

- For example, brand owners have to consider whether trademarks have been duly registered, particularly for use on digital platforms, or whether they own sufficiently well-known marks that extend to use in the virtual world. The importance of this issue was fleshed out in the case of *Hermès International et al. v Mason Rothschild*, 22-cv-00384 (SDNY), where the jury in this case decided that an NFT creator's use of the Hermes' BIRKIN mark in the title of his NFT collection constituted trademark infringement, trademark dilution and cybersquatting, notwithstanding that the Hermes BIRKIN mark was only registered for real-life goods, but not for virtual goods or NFTs. This is an important space to watch as we anticipate guidance on how regulators across the world will balance the interests of various

stakeholders who may be owners of various IA rights as developments in the virtual space continue to take shape.

- When it comes to domain names, brand owners have to be proactive in registering for domain names to protect their rights associated with their brand or risk being embroiled in numerous domain name disputes with both cyber-squatters and genuine users of similar domain names.

## NFTs

When it comes to NFTs, a distinction must be drawn between an NFT as a digital token (i.e. the smart contract codes, its unique ID, its metadata etc.) and the underlying asset that the NFT represents. Ownership of an NFT does not always represent nor grant automatic ownership of the underlying asset (such as title to the physical goods, intellectual property rights, etc.) unless there are appropriate contractual terms embedded within the NFT's metadata to tie the ownership of the actual underlying asset to the NFT. Furthermore, even with such contractual terms, different jurisdictions hold different stances as to the legality of blockchain ledgers. For example, the NFT of Jack Dorsey's tweet was auctioned on the Valuables platform. The NFT was characterised by Valuable as "an autographed certificate of the tweet" and it was made clear that the purchase of the NFT did not transfer any copyright or commercial right in the tweet to the buyer.

To add another layer of complexity to this issue, retailers and traders will have to consider the tricky subject of IP in NFTs. After all, the concept of "ownership" in NFTs is markedly different from the traditional understanding of "ownership". The scope of rights attached to the NFT will have to be thoroughly explored, and any licensing or transfer agreement would have to be carefully structured to comprehensively address the allocation of such rights.

NFTs are minted through "smart contracts", which essentially assign ownership and reassign it when sold. While such contracts are currently fairly simple, creators can include any terms that are then captured in the blockchain. They can ostensibly be used to address the grant of IP rights involved in the sale of an NFT, including the IP assignment and licensing.

After determining the scope of rights obtained, the issue then turns to how such rights can be enforced. For NFTs,

copyright holders may seek enforcement against those who have minted their copyrighted works for sale as NFTs. Outside of copyrighted material, enforcement may also be sought against those minting or selling NFTs that bear likeness to an individual without their consent.

It should also be considered who enforcement may be sought against. Individuals minting or selling NFTs that are in breach of IP rights may of course be liable, but other parties involved in the process may be found accountable as well. For example, there have been instances of NFT platforms being held liable for allowing users to mint a licensed artwork without the necessary due diligence.

### Digital Assets & Rights Management

On top of the issue of "ownership" of IA, a key focus for businesses and individuals will be digital asset management to protect the security of the assets. This would include the need for advice and services relating to digital asset and NFT securitisation, virtual real estate asset protection, gaming loot commercialisation, etc.

A challenge with rights management in the metaverse is that digital assets are often created and used by multiple users within a shared environment. As such, managing the ownership and usage rights of digital assets can become complex. In this regard, blockchain technology may be a possible solution, as it allows for the creation of secure and decentralised systems for managing ownership and usage rights.

In Singapore, IPOS has, in its vision for the future of intangible assets such as NFTs, put forth a strategy report for the year 2030 to become a global hub for IA activities. In that regard, we can see that there are steps taken by authorities in the IP industry to tackle such legal questions on IA. Anyone, businesses or individuals alike, who wishes to stay on top of the game would do well to keep abreast of such key concepts of ownership and securitisation.



# Finance and Payments

*While finance and payments form the bedrock of the commercial machinery, the very nature of money has been rapidly changing. Payments are becoming increasingly digital, cryptocurrencies are becoming progressively more established, and financial services are swiftly moving online.*



Blockchain technology is thus vital, and its continued development is unavoidable. The digital economy depends largely on its ability to support commercial activity, including the sale and purchase of virtual goods and services and the facilitation of digital trades. The commercial side of the digital world, including the metaverse, thus cannot function without electronic transactions, which in turn requires the speed and security of blockchain and blockchain platforms. This distributed ledger system allows ownership of assets to be recorded and verified, and for irrevocable peer-to-peer transactions to take place.

## Money in the Digital World

But how is money in the digital world expected to operate? Just as physical cash is increasingly phased out in favour of digital payments, traditional currencies are also expected to shift towards digital currencies. Cryptocurrencies are proliferating and gaining legitimacy, with major financial institutions already accepting crypto payments. The growing number of crypto exchanges and

investing platforms also demonstrates the commercial appetite for cryptocurrencies.

In a parallel lane, governments can also be seen to be embracing cryptocurrencies as the next logical evolution of finance. Countries such as China, Japan, Sweden and Nigeria have commenced trials for central bank digital currencies, while the Bahamas has moved ahead to release its own central bank digital currency.

On a related note, tokenisation has become somewhat a buzzword for the metaverse. Assets and items of value, including in-game and virtual assets, are capable of being tokenised, i.e. represented digitally through a smart contract on a blockchain. Such assets will likely play a part in the digital finance and payment framework.

## Financial Institutions and Payment Platforms

Banking and finance institutions will thus have to be able to adapt their systems to be able to process



cryptocurrencies and crypto payments, which are likely to become the transaction medium of choice. Some banks are already planning for virtual banking branches, decentralised finance and digital twins.

Similarly, payment platforms will have to be able to handle crypto and tokenised payment systems so as to be capable of facilitating digital transactions. Platforms which do not keep pace are likely to be left behind and excluded from the digital economy entirely.

### Regulatory Controls

The key issue in the area of finance and payments will be that of regulation and compliance. Financial institutions would be aware that the industry is one of the most heavily regulated by governments and authorities, and this is unlikely to be any different when applied to the digital economy.

### Emerging Regulation

With regard to cryptocurrencies and digital payments, regulators are likely to be seeking to manage certain key risks, including: (i) money laundering and terrorism financing; (ii) technology and cyber risks; (iii) consumer protection; and (iv) financial stability. Digital asset-related service providers should thus expect to see the emergence of legislation, regulation and guidelines in these areas, and should expect to incur obligations relating to risk assessment of products and technologies, customer due diligence requirements, and cyber hygiene standards.

Under Singapore's licensing regime, licenses and approvals have already been granted to a number of digital payment tokens service providers, including global stablecoin players and established financial institutions. The licensing framework subjects licensees to certain regulatory obligations, including some of the risk management obligations discussed above.

### Evolving Rules

One of the concerns raised in this regard is the speed at which cryptocurrencies and tokenised payment systems are advancing. The process of legislative development is usually far more conservative, hence the risk that legislation and regulation will encounter difficulty in keeping pace with technological advancement. Such laws will have to undergo continuous updating to keep

up with the rapid changes so as to ensure controlled governance of the finance and payment sector. Members of the industry will thus have to keep themselves updated on current and impending changes in the law so as to ensure preparedness and compliance with the relevant regulations.

On the issue of tokenisation, businesses should also be conscious of the legal categorisation of tokens, as this would affect the regulations they must comply with and the restrictions on their proposed activities. For example, does a token qualify as a security or other type of regulated instrument under relevant laws? This is particularly pertinent for fungible tokens.

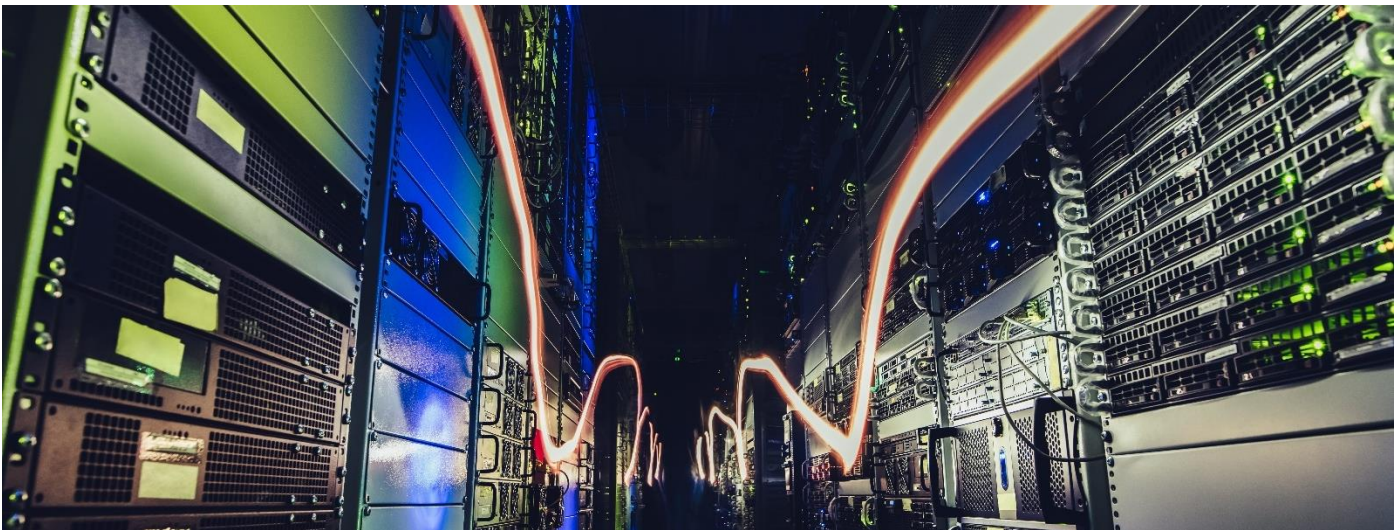
In Singapore, the Monetary Authority of Singapore regulates digital assets-related services and service providers on an activity basis – Digital assets representing a security are regulated as capital market products under the Securities and Futures Act, and a digital asset used as a means of payment are regulated as a digital payment token under the Payment Services Act.

### Jurisdiction

Going back to the familiar issue of jurisdiction, cross-border payments and transactions are expected to be part and parcel of digital commerce. However, difficulties may arise from the varying treatment of cryptocurrencies and digital payment in different jurisdictions. While standardisation and collaboration would of course be optimal, it remains to be seen how jurisdictions may work together to standardise the framework for digital finance and payments, particularly in the metaverse. A first-mover in this regard is the European Union, which has proposed the European Commission Markets in Crypto-Assets Regulation, a special dedicated regime for crypto-asset providers in the European Union, making it the first international bloc to do so. While it has yet to be implemented, it would serve to limit the offering of cryptocurrency and the operation of crypto exchanges to licensed providers.

# Infrastructure and Sustainability

*The breakneck pace of digitalisation and the development of the metaverse represent an extension of the real world and, much like the real world, will also require its own infrastructure. The sheer scale of the digital economy and the speed of its growth means that the infrastructure demands will be similarly extensive.*



The infrastructure requirements of the digital world may create a parallel industry spanning different sectors, all of which have a key role to play in setting up and maintaining the foundations upon which it is built.

## HARDWARE

- The digital economy would need to be supported by the necessary hardware.
- This would include server capacities, critical technologies, and augmented reality / display.
- Following from this, there would also be the accompanying energy requirements for processors.

## DATA AND CONNECTIVITY

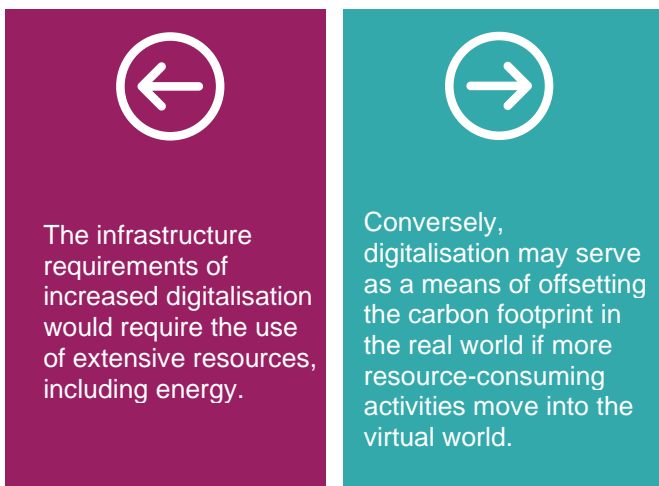
- The operation of the digital economy will need to be supported by the development of appropriate wireless communication technologies. The development of a 6G network is thus vital.
- The network must be able to handle massive concurrent streams of data, and must be both fast and stable.
- The data-handling requirements will also require the establishment of massive data centres.

## CORPORATE FRAMEWORK

- The functionality of the digital economy relies on the seamless integration of platforms, products and services, both virtual and real world.
- This would require a great degree of collaboration between technology companies and traditional companies

In addition, the advancement of digitalisation may create new opportunities in sustainability, which is quickly becoming a prime factor in business decisions and a priority in international policy. It will thus inevitably be a factor in the building of the relevant infrastructure.

In this regard, the sustainability opportunities may not be so straightforward, with the potential to head in drastically different directions – will it lead to greater consumption of resources, or will its advantages of innovation lead to greater solutions?



The above sectors are rife with opportunities for businesses in the relevant industries to capitalise on. Here, we look at the various legal issues associated with participating in the physical infrastructure of the digital world.

### Intellectual Property

As highlighted, the infrastructure supporting digital activity will be heavily dependent on critical technologies. This means that IP and licensing issues will come to the forefront of the issues to be considered when engaging in such technologies. Due to the immense value of the underlying IP, technology IP owners will be concerned with how to protect their rights over the technology (including through copyrights and patents, IP policing, and technological protection). Similarly, publishers and manufacturers who design and build with such technologies will have to address how to structure the licensing of the technologies for use.

### Commercial Arrangements

The digital economy lives or dies by its interconnectivity, meaning that no one platform will be able to dominate or monopolise proceedings. Establishing the necessary infrastructure is thus not a one-player game, but will require a multi-player campaign where the key players in the industry (including telcos, service providers, etc) must collaborate.

The structuring of their arrangements, both in terms of contract and corporate structure, will have to be addressed, which may be challenging given the untested nature of such cooperation. Businesses would have to look into their options and interests in terms of mergers and acquisition ("M&A") activity and ask the right questions, including: What is the appropriate vehicle for collaboration? How should one structure a joint venture? What should be addressed in a collaboration agreement between builders? What specific M&A checklist indicators are required?

### Competition

The digital economy, expansive as it may be, is ultimately based in commerce and incorporates many different markets. Competition authorities will thus likely want to ensure that there is sufficient access to products or services which are essential for effective competition in the metaverse.

It has been a feature of the digital economy that markets show a high degree of concentration. As such, takeovers and mergers can easily create a market that is effectively impenetrable to competitors. To address such risks, competition regulators are likely to undertake closer scrutiny of merger control in the context of digitalisation and the metaverse.

Parties seeking to take part in the infrastructure of the digital economy, especially if engaging in M&A or collaborative activity, should thus pay attention to the competition risks that may arise so as to assess whether they may be in breach of any regulations or if any remedial measures are necessary.

### Sustainability

As a digital and technological construct, the energy required to power the digital world will bring into relevance issues of energy and resources, such as

electricity generation and supply, water supply, etc. In order to tap into this market, operators must have an understanding of the relevant energy laws and regulations.

As they move to the metaverse and beyond, businesses should also consider how their operations may support sustainability efforts. Apart from a compliance aspect, businesses may also be able to take advantage of benefits afforded to sustainable projects, such as green financing and rebates. It may be expected that governments will impose increasingly stringent sustainability standards in the near future. Compliance with such standards in the areas of energy usage and emissions will thus be a key concern.



## Real Estate

*As individuals begin to establish their identities in the virtual sphere, the real-world concepts that they engage in will need to find an equivalent digital representation. This would include the need for a place to stay, or for a location from which to conduct work, commerce and leisure.*



The technologies supporting the virtual world are already changing the use of physical locations.

- Today, cycling enthusiasts can compete in a virtual Tour De France.
- Visitors can virtually tour the best museums.
- Accenture created its headquarters' "digital twin" and carried out virtual orientations for new employees. This global entity has carried out over 100 such events, ensuring that employees across the globe share the same unified experience.

As technology enables virtual worlds to become more realistic and allows the generation of high-fidelity digital twins, real estate investors should consider the corresponding impact on physical locations.

- In terms of office space, advances in video conferencing technology today have already reduced the necessity of face-to-face meetings, and the metaverse will bring about a further improvement

in such alternative work arrangements. For example, Microsoft is testing a version of Microsoft Teams using digital avatars where workers can share documents in the virtual world.

- Digital twins of factories and hospitals are now within technological reach, furthering the prospects of remote working.
- The tokenisation of real estate has also enabled the value of physical real estate to be converted into divisible tokens stored on a blockchain, allowing for digital ownership and transfer of fractional shares in real-world property. The lowered barriers to entry open the doors to a more accessible investment market.

What does this mean for the future of work, and how does this impact investments in real estate, particularly commercial real estate? Investors and businesses in the real estate section will have to consider these issues as they adapt to operating in the digital economy.



Investing in the virtual world has taken off as well.

- Companies building the hardware required to participate in the metaverse have attracted significant investment.
- Direct investment in virtual real estate has also picked up. Investors can buy virtual land on platforms such as SecondLife, Decentraland, and The Sandbox. Virtual real estate development companies such as Republic Realm and Tokens.com have invested millions in purchasing virtual land on these platforms.
- Such virtual spaces can serve as a doorway into further commercial opportunities, such as marketing space, rental, development, retail, and events.



There is no shortage of investment and development opportunities surrounding digital real estate.

However, investors and businesses seeking to embrace this opportunity will have to contend with issues unique to virtual real estate, including volatility, currency, and regulatory risks.

### Real Estate

One of the prime concerns may be that of the inherent volatility of the property market, which is further exacerbated by the potentially less predictable market forces in the virtual sphere. After all, the value of virtual land is intrinsically tied to the corresponding demand,

and the popularity of any given platform can sometimes be fickle.

The volatility of the digital real estate market is also likely to raise the issue of speculation. This then leads to the question of whether government regulators will seek to impose regulations and frameworks so as to control and stabilise the market.

### Regulatory Control

The market for digital real estate and tokenised real-world property is still largely based in the private sector. While this allows for a degree of flexibility in trading, it comes with the corresponding drawbacks of private investment markets, including susceptibility to fraud and the demonstrated risk of poor cybersecurity practices.

The emerging market presents an opportunity for regulators to play a role in drawing up rules and boundaries to provide for greater control and security. For example, regulators may set up a virtual registry for expression of title in virtual real estate.

### Taxation

Another issue is that of taxation, which is a key issue in real-world property. In contrast, there is currently no taxation on virtual property. This is likely due to the fact that digital real estate as a viable market is still fairly fresh, meaning that regulatory authorities may not have had the opportunity to fully consider such taxation. However, as the virtual real estate market continues to grow, governments will likely seek to introduce regulations, including taxation, so as to better manage and capitalise on the market. Investors will have to keep aware of the additional costs that may be incurred and how they may best structure their investments in this regard.

# Retail and Commerce in the Metaverse

*Retail has long been on a trajectory towards a more online presence, shifting away from physical retail outlets. It is a given assumption that online stores will exist in the metaverse, but this is likely only the starting point of the transformation of retail and commerce.*



Businesses will have to rethink fundamental concepts, including what constitutes a "store" and how products are sold. In a virtual setting, these concepts may take on a markedly different veneer. While the exact form the user experience will take is still unclear, businesses will at least have to adapt their products and services for online sale as a first step.

Retail is also set for a revolution in terms of what is being sold, going beyond hosting physical products on an online platform. Virtual ownership and possessions will gain increasing importance, be it clothing and accessories for your metaverse avatar or furniture for your virtual accommodation. Major brands have already begun releasing entire lines of virtual products, and even more have undertaken the first steps to participating in virtual retail by registering their trade marks for virtual use in the metaverse.



## Traditional Retail

- Physical retail outlets
- Real world products and services
- Physical ownership

Perhaps the best example of this is the rise of NFTs. NFTs tokenise virtual assets to make them tradeable, and their commercial legitimacy is already taking shape. While NFTs can grant value to almost anything (a tweet, an image, a sound), the early focus has been on the use of NFTs to trade artwork. For a clear example, at an auction at Christie's, the artist known as Beeple had

NFTs of his work sold for US\$69 million. NFTs have also been a hot topic in areas such as gaming and music.



### Virtual Retail

- Digital platforms and virtual stores
- Virtual products and online services
- NFTs and tokenised assets

Retailers will thus also have to drastically rethink the products that are saleable and tradeable (such as the scope of coverage of NFTs, virtual real estate, etc) so as to be able to capitalise on the opportunities provided in the virtual retail and commerce sector.

In addition to the products being sold, retailers must also address how the sale is being made. Payment processes are continually evolving, from physical to digital payments, and now progressing to tokenisation in e-commerce, which allows for greater security in digital payments by removing the need for the disclosure of sensitive payment details.

The transformation of retail also brings about a change in the legal issues that retailers have to deal with. Though the general areas of law may be familiar, the specific issues relating to virtual retail are potentially unfamiliar to the traditional retailer.

### Regulatory Control

Virtual retail, much like physical retail and online retail, will be subject to regulation. Such laws are still in the process of development, and will likely undergo further iterations to address the new issues arising with each stage of transition.

For example, in Singapore, new regulations and guidelines are continually being released for online retailers and retail platforms in an effort to keep pace with the changing practices of retailers and the evolving

measures needed to afford adequate protection to the consumer. An example of this would be Technical Reference 76, which is the first national standard on guidelines for e-commerce transactions. Launched by Enterprise Singapore and the Singapore Standards Council, Technical Reference 76 serves as a practical guide for e-retailers who sell directly to customers online, as well as online intermediaries such as e-marketplaces, providing comprehensive end-to-end coverage of the e-commerce transaction process.

The tokenisation of commerce and the shift away from physical payments also means that the legal framework for conducting trade needs to adapt to the new circumstances, whether through the development of legislative frameworks or by parties entering into contractual arrangements. For example, the UNCITRAL Model Law on Electronic Transferable Records was created to enable the legal use of electronic transferrable records both domestically and cross-border. This would include electronic bills of lading which, similar to NFTs, operate via blockchain technology. Countries can adopt such model laws to facilitate the conduct of tokenised trade.

For example, in Singapore, the TradeTrust framework was launched to enable interoperability of electronic trade documents across digital platforms. It allows end users to digitally endorse, exchange and verify documents used in cross-border trade and effect title transfer.

Similar to the topic of finance and payments above, members of the industry will have to keep themselves updated on current and impending changes in the law so as to ensure preparedness and compliance with the relevant regulations.

### Competition

Competition law is an important topic in the area of retail and commerce. Further, across the world, competition authorities and legislative bodies have made digital markets a priority area for enforcement. The growth of the metaverse and digitisation will thus come under close scrutiny from competition regulators.

Competition regulators will naturally seek to keep markets open and free for companies to do business with consumers. This is particularly pertinent due to the

nature of online commerce, in which a critical mass of other users on the same platform is likely to lead to the tipping of the market due to benefits to users and businesses. Competition authorities will also be on the lookout for self-preferencing practice by digital platforms. Such practices may distort competition and cause third-party businesses to be increasingly dependent on the platform's services.

# Privacy, Data Protection and Data Governance

*In the past years, privacy and data protection has not only become a prime concern for businesses and individuals but has progressed to become an industry in itself. The dangers associated with personal data have risen at an alarming rate, and government regulators are increasingly imposing on businesses heightened obligations relating to data protection. Businesses have thus had to develop their data protection capabilities, both technologically and operationally, so as to ensure compliance.*



Information is its own currency, and the sheer amount of personal data being shared online brings a host of risks. Privacy and data protection will thus be even more pertinent in the digital economy, including the metaverse, where the personalisation of the experience will require the collection of huge amounts of personal data. Mediating devices for the metaverse such as VR headsets can provide greater opportunities for enhanced data harvesting and user surveillance, from which more sensitive inferences on the user may be drawn. Further, as the digital economy depends on the seamlessness of transition between different services and activities, the sharing of information between companies will involve the constant transfer of such data sets.

The issue of privacy is further complicated by the multiplicity of identities in the virtual world; a user's existence in the virtual world is necessarily a second

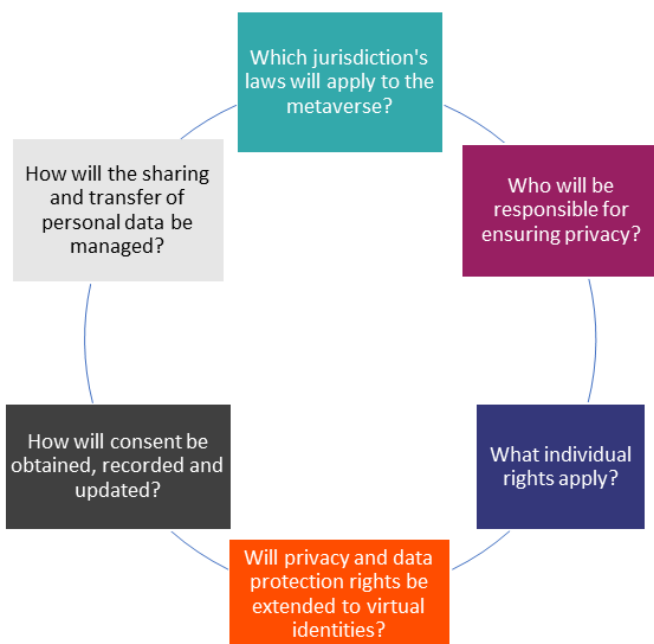
persona, and each user can have numerous digital identities. While a user's real-world identity is the source of their personal information, their virtual identity may also give rise to a new and additional source of personal information that must be protected, which then gives rise to difficult questions on the boundaries of protection and what falls within personal data. Would this include information on the individual's avatar, or must it relate directly to the individual?

It would thus be greatly advantageous for businesses to tackle issues of privacy and data protection early, capitalising on the opportunity for preliminary action. This would include addressing the areas of policy, practice, and technological support.



## Data Protection

Data protection laws are – in the grand scheme of national legislation – still fairly young, and are in the process of constant development to deal with new threats and concerns. Such laws will also have to adapt to the new issues and practicalities brought about by the metaverse. While the laws of different jurisdictions may vary, there are certain concepts which are generally similar across the board. The questions arising from the advent of the metaverse would include:



On the topic of who is responsible for ensuring privacy, the question is complicated by the number of parties involved in the chain of personal data collection and use, including VR device manufacturers, platforms, service providers, and intermediaries. The issue is given further dimension by differences in data protection laws across jurisdictions. For example, the European Union General Data Protection Regulation allocates responsibility to the data controller (the entity which determines the means of processing the personal data); this broad notion of control may not be identically adopted in other jurisdictions. The exceptions to data protection obligations, such as for individual users acting in their personal/domestic capacities, may also differ in scope.

In Singapore, the protection of personal data is governed by the Personal Data Protection Act ("**PDPA**"), which sets out a baseline standard for protection, and comprises various requirements on the collection, use,

disclosure, and care of personal data. While its provisions do not explicitly address virtual application, the general principles are likely to be applicable in the context of managing personal data in the metaverse. First introduced in 2012, the PDPA has undergone (and continues to undergo) constant development to adapt to changing circumstances.

## LegalTech

Whatever the form taken by the data privacy laws applying to the metaverse, businesses will have to ensure compliance with the rules. LegalTech service providers will thus be vital to businesses in this regard, as businesses should seek advice on:

- Privacy policies and how they should be updated to allow for concurrent use of data in the real world and the digital economy;
- The internal processes necessary to deal with consent, notification, access and correction requests, and care of personal data;
- Technological solutions to ensuring the necessary level of protection of personal data; and
- Issues of data portability.

## Cybersecurity and Cybercrimes

*Technology is not the only thing in a constant state of development; there is a flip side to every coin, and the darker aspect of technological advancement is the perpetration of increasingly sophisticated crimes. No longer constrained to the physical world, theft is far more pervasive in the digital realm, with hackers accessing personal information and gaining entry to bank accounts and e-wallets, and new scams being created every day.*



As more commercial activities and transactions take place in the digital economy, and more assets are stored on digital platforms, it may be inevitable that cybercrime will follow the trail. This may take many different forms, including direct cyberattacks, phishing scams, etc.

Cybersecurity will thus be of key importance to businesses and users alike. Although cybercrimes are already a commonplace threat in the digital world, it is a concern that many businesses and their employees are still not equipped with the necessary cybersecurity tools, policies and practices, and are even less prepared to face the new and advanced threats of cybercrime in the context of the metaverse and beyond.

Companies may be familiar with existing crimes, hacks and scams, but the shift of commercial activity into the virtual world – itself a creature of innovation and development – means that we may anticipate the creation of new and specific hacks (e.g. abuse of digital assets, identity theft, etc.).

The potential proliferation of cybercrime also means that businesses should be especially aware of anti-money laundering and combating the financing of terrorism ("AML"). With more pervasive scams and tactics consistently being developed, companies should ensure that they are not unwittingly facilitating such crimes or the processing of ill-begotten funds. As regulators continue to enhance and adapt their AML frameworks and regulations to deal with emerging threats, businesses must ensure that they are in compliance with the relevant obligations and standards.

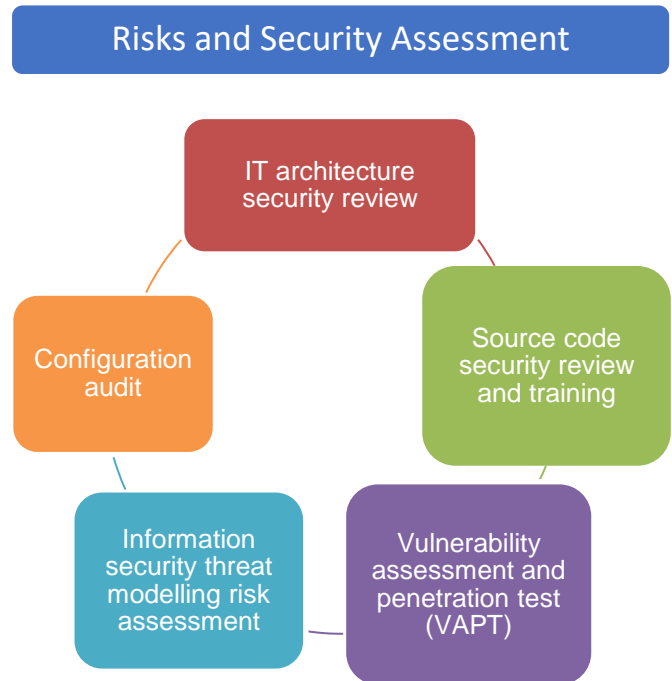
Businesses would thus be well advised to get a head start in implementing the necessary cybersecurity and AML solutions to duly protect themselves.

### LegalTech

In this regard, it is important for businesses to seek the input of LegalTech service providers. Led by highly

experienced technical experts in the field of security services and consultancy, Rajah & Tann Cybersecurity is a market leader in providing comprehensive pre and post incident security services, offering end-to-end services that cover the entire risk management lifecycle and ensure a robust cybersecurity solutions strategy.

Rajah & Tann Cybersecurity's suite of services include the following:



# Ethics

*The human condition necessitates the consideration of issues of ethics in any given endeavour. For businesses, this is not just a matter of morality, but also of corporate social responsibility. With regard to digitalisation and the metaverse, the unexplored developments and use of technology mean that we may anticipate the emergence of new and complex ethical issues.*



One of the areas of interest where technology and ethics cross paths is that of Artificial Intelligence ("AI"). The rapid growth and implementation of Generative AI systems such as Bard and ChatGPT in daily business activities heightens the need for vigilance and urgent regulatory intervention in this area. The use of AI and machine learning will play a large role in the metaverse, such as through AI 'humans' or intuitive interfacing, and can lead to great efficiencies and advancement. Businesses have already been capitalising on AI tools in their operations, easing the burden of certain rote tasks. The areas of use for AI in business functions include data analysis, customer service, hiring and performance assessments, and process automation.

However, this raises the question of the ethical compliance of AI systems, including:

## OWNERSHIP RIGHTS

- AI programs may be able to independently generate creative works.
- Who has ownership of works generated by AI programs: the program user, the programmer or in the AI itself?

## ALGORITHMIC BIAS

- The algorithm or machine learning of the program may result in adverse bias and discrimination.
- Who would be responsible: the programmer, the parties feeding the training data, or the organisation implementing the technology?

## MISUSE AND ABUSE



- The supporting technology may be misused in numerous ways, including deepfakes, hacked avatars, abuse of avatars, and manipulated objects.
- What remedies and rights will victims be able to rely on?
- Will such acts fall foul of specific offences?

AI operators will thus need to consider their internal processes and governance in relation to such ethical concerns. Taking a cue from the issues highlighted above, this would include a consideration of:

- **The scope for bias in systems and outputs** – This would involve a comprehensive understanding of the AI program, such as the algorithm employed, the criteria used, and adverse impact assessments conducted.
- **The quality and nature of training data** – The machine learning of an AI program is dependent on the training data, meaning that its function is susceptible to any inaccuracies or prejudice in the training data.
- **Systems resilience and accuracy** – The resilience of an AI program, or its ability to adapt to risks, may be compromised by a variety of failures in development or operation.
- **Human oversight and intervention** – Businesses and organisations are unlikely to be able to abdicate all responsibility for decisions or actions taken by AI programs; some degree of human oversight (and remedial intervention if necessary) will still be required.

# Dispute Resolution

*It is inevitable that wherever individuals or businesses interact, there will be a divergence of interests leading to disagreements and disputes. This is likely also true for interactions in the metaverse.*

*As digitalisation changes how we interact and how the commercial world operates, the area of dispute resolution will also see new evolution. The most obvious impact would be the emergence of new legal issues and untested disputes and claims. Another effect will be how dispute resolution is conducted. As processes continue to move from the real world, it is likely that dispute resolution proceedings (be it litigation arbitration or mediation) will also move online and into the virtual world.*



## Legal issues

- Metaverse interdependency
- Token specific disputes
- Avatar legal rights



## Dispute resolution mechanisms

- Virtual mediation, arbitration, litigation
- Cross-jurisdiction cooperation
- Metaverse-based non-jurisdiction specific forum

## Legal Issues

With such changes will come new efficiencies, as well as new challenges.

Businesses facing legal disputes will require legal counsel that is familiar with and on top of the evolving legal concepts in the digital economy and the metaverse. Legal service providers which are tapped into the technology industry will thus be well-placed to advise on the new range of disputes.

In Singapore, the Courts have recently seen a number of landmark decisions which demonstrate the novelty of issues which may arise relating to Data and Digital Economy, such as the legal recognition of rights in the online environment, and the enforcement of orders against online personas.

- In ***CLM v CLN and others* [2022] SGHC 46**, the Singapore High Court granted the first reported freezing injunction against "persons unknown" in Singapore for S\$9.6 million worth of cryptocurrency assets.
- In ***Janesh s/o Rajkumar v Unknown Person* [2022] SGHC 264**, the Singapore High Court issued a landmark decision granting an injunction over a Bored Ape NFT, recognising that NFTs are capable of giving rise to proprietary rights which can be protected by an injunction. The Court allowed the application despite the fact that the Claimant only knew the Defendant by his online handle, and further demonstrated the adaptability of its processes by allowing the summons to be served via the Defendant's Twitter, Discord, and cryptocurrency wallet address.

## Dispute Resolution Mechanisms

Disputants would also be well served by legal counsel that has the technological capabilities to support and take advantage of the new processes that may arise. Disputants should be able to duly manage procedural issues such as meta e-discovery and forensics, online dispute resolution proceedings, etc.

# Our Achievements

Rajah & Tann Asia has been named as a leading Technology, Media and Telecommunications Practice across several different jurisdictions across South East Asia by major legal ranking journals, including but not limited to:

|  |   |  |
|--|---|--|
| <p><b>Chambers Asia-Pacific 2023</b></p>  <p><b>Band 1, Technology, Media, Telecoms</b><br/>Rajah &amp; Tann Asia</p> | <p><b>The Legal 500 Asia Pacific 2023</b></p>  <p><b>Tier 1, TMT</b><br/>Rajah &amp; Tann Asia</p>   | <p><b>Asialaw Profiles 2023</b></p>  <p><b>Outstanding, Technology and Telecommunications</b><br/>Rajah &amp; Tann Asia</p> |
| <p><b>Global Data Review 100 2023</b></p>  <p><b>Top 100 Data Law Firms Globally</b><br/>Rajah &amp; Tann Asia</p>  | <p><b>FT Innovative Lawyers Awards Asia</b></p>  <p><b>2023</b><br/><i>Winner:</i><br/><b>Most Innovative SE Law Firm in Asia Pacific</b><br/><b>Most Innovative Lawyers in Cyber Security &amp; Data Governance</b></p> <p><i>Shortlisted:</i><br/><b>Most Innovative Lawyers in Digital Assets</b><br/><b>Most Innovative Lawyers in Innovation in Training &amp; Development</b></p> <p><b>2020</b><br/><b>Leadership in IT Strategy</b><br/><b>Top 20 Most Innovative Firms in Asia Pacific</b></p> |  |



## Our Achievements: Individual Accolades

The members of our Rajah & Tann Asia Technology, Media and Telecommunications team have also been individually recognised in various legal ranking journals, including but not limited to:

| Chambers Asia-Pacific 2023  | The Legal 500 Asia Pacific 2023  | Asialaw Profiles 2023   |
|---|--|---|
|  <p><b>Chambers<br/>TOP RANKED<br/>Asia-Pacific<br/>2023</b></p> <p><b><u>Technology, Media, Telecoms</u></b></p> <p><i>Singapore:</i><br/><b>Rajesh Sreenivasan, Band 1<br/>Steve Tan, Band 2<br/>Lionel Tan, Band 4</b></p> <p><i>Malaysia:</i><br/><b>Deepak Pillai, Band 1<br/>Intan Haryati, Band 2<br/>Kuok Yew Chen, Band 2</b></p> <p><i>Indonesia:</i><br/><b>Zacky Zainal, Band 1<br/>Iqsan Sirie, Up and Coming</b></p> |  <p><b>The<br/>LEGAL<br/>500<br/>ASIA PACIFIC<br/>TOP TIER<br/>2023</b></p> <p><b><u>TMT</u></b></p> <p><i>Singapore:</i><br/><b>Rajesh Sreenivasan, Leading Lawyer<br/>Steve Tan, Leading Lawyer<br/>Benjamin Cheong, Next Gen Lawyer</b></p> <p><i>Malaysia:</i><br/><b>Deepak Pillai, Hall of Fame<br/>Intan Haryati, Hall of Fame<br/>Kuok Yew Chen, Hall of Fame<br/>Anissa Anis, Next Gen Lawyer<br/>Yong Shih Han, Next Gen Lawyer</b></p> <p><i>Indonesia:</i><br/><b>Zacky Zainal, Leading Lawyer</b></p> <p><i>Vietnam:</i><br/><b>Vu Thi Que, Leading Lawyer</b></p> |  <p><b>asialaw<br/>LEADING<br/>LAWYERS<br/>DISTINGUISHED<br/>PRACTITIONER<br/>2023</b></p> <p><b><u>Technology and<br/>Telecommunications</u></b></p> <p><i>Singapore:</i><br/><b>Rajesh Sreenivasan, Elite<br/>Practitioner<br/>Steve Tan, Distinguished<br/>Practitioner</b></p> <p><i>Malaysia:</i><br/><b>Deepak Pillai, Elite<br/>Practitioner</b></p> |

Who's Who Legal 2023



Data Privacy & Protection

Rajesh Sreenivasan, Global Elite Thought Leader  
Steve Tan, Recommended

Data Security

Steve Tan, Recommended

Fintech & Blockchain

Deepak Pillai, Recommended

Information Technology

Lau Kok Keng, Recommended  
Rajesh Sreenivasan, Recommended

Telecoms & Media

Rajesh Sreenivasan, Recommended

Southeast Asia – Data

Lau Kok Keng, Recommended  
Rajesh Sreenivasan, Recommended  
Steve Tan, Recommended

FT Innovative Lawyers Awards Asia



2023

*Shortlisted:*

Patrick Ang – Innovative Individual Leaders

2019

Steve Tan, Top 10 Legal Innovators  
for Asia Pacific Region

2018

Rajesh Sreenivasan, Top 10 Pioneers  
of New Legal Thinking

# Our Regional Contacts

## Digitalisation and TMT

### Rajesh Sreenivasan

Rajah & Tann Singapore LLP  
D +65 6232 0751  
E [rajesh@rajahtann.com](mailto:rajesh@rajahtann.com)

### Steve Tan

Rajah & Tann Singapore LLP  
D +65 6232 0786  
E [steve.tan@rajahtann.com](mailto:steve.tan@rajahtann.com)

### Benjamin Cheong

Rajah & Tann Singapore LLP  
D +65 6232 02738  
E [benjamin.cheong@rajahtann.com](mailto:benjamin.cheong@rajahtann.com)

### Lionel Tan

Rajah & Tann Singapore LLP  
D +65 6232 0752  
E [lionel.tan@rajahtann.com](mailto:lionel.tan@rajahtann.com)

### Tanya Tang

Rajah & Tann Singapore LLP  
D +65 6232 0298  
E [tanya.tang@rajahtann.com](mailto:tanya.tang@rajahtann.com)

## Ethics; Dispute Resolution

### Rajesh Sreenivasan

Rajah & Tann Singapore LLP  
D +65 6232 0751  
E [rajesh@rajahtann.com](mailto:rajesh@rajahtann.com)

### Jansen Chow

Rajah & Tann Singapore LLP  
D +65 6232 0624  
E [jansen.chow@rajahtann.com](mailto:jansen.chow@rajahtann.com)

### Kuok Yew Chen

Christopher & Lee Ong  
D +60 3 2273 1919 / +60 3 2267 2699  
E [yew.chen.kuok@christopherleeong.com](mailto:yew.chen.kuok@christopherleeong.com)

### Tan Yi Li

Christopher & Lee Ong  
D +60 3 2273 1919 / +60 3 2267 2691  
E [yi.li.tan@christopherleeong.com](mailto:yi.li.tan@christopherleeong.com)

### Rubini Murugesan

Christopher & Lee Ong  
D +60 3 2273 1919 / +60 3 2267 2616  
E [rubini.murugesan@christopherleeong.com](mailto:rubini.murugesan@christopherleeong.com)

### Ahmad Fikri Assegaf

Assegaf Hamzah & Partners  
D +62 21 2555 7880  
E [ahmad.asegaf@ahp.id](mailto:ahmad.asegaf@ahp.id)

## Finance & Payments

### Regina Liew

Rajah & Tann Singapore LLP  
D +65 6232 0456  
E [regina.liew@rajahtann.com](mailto:regina.liew@rajahtann.com)

### Kuok Yew Chen

Christopher & Lee Ong  
D +60 3 2273 1919 / +60 3 2267 2699  
E [yew.chen.kuok@christopherleeong.com](mailto:yew.chen.kuok@christopherleeong.com)

### Tracy Wong

Christopher & Lee Ong  
D +60 3 2273 1919 / +60 3 2267 2653  
E [tracy.wong@christopherleeong.com](mailto:tracy.wong@christopherleeong.com)

### Zacky Zainal Husein

Assegaf Hamzah & Partners  
D +62 21 2555 7800  
E [zacky.husein@ahp.id](mailto:zacky.husein@ahp.id)

### Ahmad Fikri Assegaf

Assegaf Hamzah & Partners  
D +62 21 2555 7880  
E [ahmad.asegaf@ahp.id](mailto:ahmad.asegaf@ahp.id)

### Indira Yustikania

Assegaf Hamzah & Partners  
D +62 21 2555 7800  
E [indira.yustikania@ahp.id](mailto:indira.yustikania@ahp.id)

## Media; Intangible Assets and Rights Management

### Lau Kok Keng

Rajah & Tann Singapore LLP  
D +65 6232 0765  
E [kok.keng.lau@rajahtann.com](mailto:kok.keng.lau@rajahtann.com)

### Chandra Hamzah

Assegaf Hamzah & Partners  
D +62 21 2555 7800  
E [chandra.hamzah@ahp.id](mailto:chandra.hamzah@ahp.id)

**Zacky Zainal Husein**

Assegaf Hamzah & Partners  
D +62 21 2555 7800  
E [zacky.husein@ahp.id](mailto:zacky.husein@ahp.id)

**Anissa Maria Anis**

Christopher & Lee Ong  
D +60 3 2273 1919 / +60 3 2267 2750  
E [anissa.anis@christopherleeong.com](mailto:anissa.anis@christopherleeong.com)

**Sri Sarguna Raj**

Christopher & Lee Ong  
D +60 3 2273 1919 / +60 16 263 9727  
E [sri.sarguna.raj@christopherleeong.com](mailto:sri.sarguna.raj@christopherleeong.com)

**Supawat Srirungruang**

R&T Asia (Thailand)  
D +66 2 656 1991  
E [nuttaphol.a@rajahtann.com](mailto:nuttaphol.a@rajahtann.com)

**Saroj Jongsaritwang**

R&T Asia (Thailand)  
D +66 2 656 1991  
E [saroj.jongsaritwang@rajahtann.com](mailto:saroj.jongsaritwang@rajahtann.com)

**Infrastructure & Sustainability; Real Estate****Norman Ho**

Rajah & Tann Singapore LLP  
D +65 6232 0514  
E [norman.ho@rajahtann.com](mailto:norman.ho@rajahtann.com)

**Benjamin Tay**

Rajah & Tann Singapore LLP  
D +65 6232 0375  
E [benjamin.st.tay@rajahtann.com](mailto:benjamin.st.tay@rajahtann.com)

**Shemane Chan**

Rajah & Tann Singapore LLP  
D +65 6232 0285  
E [shemane.chan@rajahtann.com](mailto:shemane.chan@rajahtann.com)

**Chester Toh**

Rajah & Tann Singapore LLP  
D +65 6232 0220  
E [chester.toh@rajahtann.com](mailto:chester.toh@rajahtann.com)

**Terence Quek**

Rajah & Tann Singapore LLP  
D +65 6232 0277  
E [terence.quek@rajahtann.com](mailto:terence.quek@rajahtann.com)

**Favian Tan**

Rajah & Tann Singapore LLP  
D +65 6232 0626  
E [favian.tan@rajahtann.com](mailto:favian.tan@rajahtann.com)

**Lim Siaw Wan**

Christopher & Lee Ong  
D +60 3 2273 1919 / +60 3 2267 2731  
E [siawwan.lim@christopherleeong.com](mailto:siawwan.lim@christopherleeong.com)

**Sirie Muhammad Iqsan**

Assegaf Hamzah & Partners  
D +62 21 2555 7805  
E [iqsan.sirie@ahp.id](mailto:iqsan.sirie@ahp.id)

**Eko Basyuni**

Assegaf Hamzah & Partners  
D +62 21 2555 7805  
E [eko.basyuni@ahp.id](mailto:eko.basyuni@ahp.id)

**Privacy, Data Protection & Data Governance;  
Cybersecurity & Cyber Crime****Steve Tan**

Rajah & Tann Singapore LLP  
D +65 6232 0786  
E [steve.tan@rajahtann.com](mailto:steve.tan@rajahtann.com)

**Thong Chee Kun**

Rajah & Tann Singapore LLP  
D +65 6232 0156  
E [chee.kun.thong@rajahtann.com](mailto:chee.kun.thong@rajahtann.com)

**Deepak Pillai**

Christopher & Lee Ong  
D +60 3 2273 1919 / +60 3 2267 2675  
E [deepak.pillai@christopherleeong.com](mailto:deepak.pillai@christopherleeong.com)

**Sirie Muhammad Iqsan**

Assegaf Hamzah & Partners  
D +62 21 2555 7805  
E [iqsan.sirie@ahp.id](mailto:iqsan.sirie@ahp.id)

**Logan Leung**

Rajah & Tann LCT Lawyers  
D +84 28 3821 2382  
E [logan.leung@rajahtannlct.com](mailto:logan.leung@rajahtannlct.com)

**Supawat Srirungruang**

R&T Asia (Thailand)  
D +66 2 656 1991  
E [nuttaphol.a@rajahtann.com](mailto:nuttaphol.a@rajahtann.com)

**Wong Onn Chee**

Rajah & Tann Technologies  
D +65 9838 7930  
E [onnchee@rtcyber.com](mailto:onnchee@rtcyber.com)



## Retail & Commerce

### **Kala Anandarajah**

Rajah & Tann Singapore LLP

D +65 6232 0111

E [kala.anandarajah@rajahtann.com](mailto:kala.anandarajah@rajahtann.com)

### **Eko Basyuni**

Assegaf Hamzah & Partners

D +62 21 2555 7805

E [eko.basyuni@ahp.id](mailto:eko.basyuni@ahp.id)

### **Kuok Yew Chen**

Christopher & Lee Ong

D +60 3 2273 1919 / +60 3 2267 2699

E [yew.chen.kuok@christopherleeong.com](mailto:yew.chen.kuok@christopherleeong.com)

### **Tracy Wong**

Christopher & Lee Ong

D +60 3 2273 1919 / +60 3 2267 2653

E [tracy.wong@christopherleeong.com](mailto:tracy.wong@christopherleeong.com)

### **Logan Leung**

Rajah & Tann LCT Lawyers

D +84 28 3821 2382

E [logan.leung@rajahtannlct.com](mailto:logan.leung@rajahtannlct.com)

Rajah & Tann Asia is a network of legal practices based in Asia.

Member firms are independently constituted and regulated in accordance with relevant local legal requirements. Services provided by a member firm are governed by the terms of engagement between the member firm and the client.

This guide is solely intended to provide general information and does not provide any advice or create any relationship, whether legally binding or otherwise. Rajah & Tann Asia and its member firms do not accept, and fully disclaim, responsibility for any loss or damage which may result from accessing or relying on this guide.

# Disclaimer

Rajah & Tann Asia is a network of member firms with local legal practices in Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. Our Asian network also includes our regional office in China as well as regional desks focused on Brunei, Japan and South Asia. Member firms are independently constituted and regulated in accordance with relevant local requirements.

The contents of this publication are owned by Rajah & Tann Asia together with each of its member firms and are subject to all relevant protection (including but not limited to copyright protection) under the laws of each of the countries where the member firm operates and, through international treaties, other countries. No part of this publication may be reproduced, licensed, sold, published, transmitted, modified, adapted, publicly displayed, broadcast (including storage in any medium by electronic means whether or not transiently for any purpose save as permitted herein) without the prior written permission of Rajah & Tann Asia or its respective member firms.

Please note also that whilst the information in this publication is correct to the best of our knowledge and belief at the time of writing, it is only intended to provide a general guide to the subject matter and should not be treated as legal advice or a substitute for specific professional advice for any particular course of action as such information may not suit your specific business and operational requirements. You should seek legal advice for your specific situation. In addition, the information in this publication does not create any relationship, whether legally binding or otherwise. Rajah & Tann Asia and its member firms do not accept, and fully disclaim, responsibility for any loss or damage which may result from accessing or relying on the information in this publication.