the global voice of the legal profession

IBA Intellectual Property, Communications and Technology Law Committee

Digital Regulations in the Metaverse Era

SINGAPORE

Regional Coordinators:
Angela Flannery *Quay Law Partners, Sydney*
Yoshifumi Onodera *Mori Hamada & Matsumoto, Tokyo*

Data

Lam Chung Nian *WongPartnership, Singapore*
Huey Lee *WongPartnership, Singapore*

Q 1. Are there any data (personal and non-personal) policies, strategies or regulations applicable to the metaverse in your jurisdiction?

The Personal Data Protection Act 2012 (PDPA) established a general personal data protection regime in Singapore which is enforced and administered by the Personal Data Protection Commission (PDPC). This is a consent-based regime where an individual's consent is generally required for any collection, use or disclosure of their personal data, unless there are applicable exceptions.

The PDPA generally takes a technology-neutral approach in regulating personal data and applies to the collection, use and disclosure of personal data regardless of the medium on which the data is stored or processed. The PDPC regularly publishes guidelines addressing emerging technological developments and new data processing scenarios. Some of the issues that the PDPC may pay particular attention to in relation to the metaverse include digital avatars and Big Data:[1]

- digital avatars: if users' digital personas and avatars in the metaverse are a close approximation of their real-world selves, such personas and avatars could potentially be considered personal data; and
- big data: metaverse platforms are likely to process large volumes of data in light of their immersive nature, as such Big Data may include biometric and activity data from body sensors. Considering the scale and sensitivity of the data, it will be important to ensure that it is securely protected and properly used.

The PDPA provides for a baseline standard of protection for personal data which complements common law requirements and sector and activity-specific regulatory frameworks, such as those applicable to the healthcare and medical sectors, financial sector, confidential information and official secrets. Organisations must therefore comply with the PDPA in addition to these other relevant laws (when applicable) when handling personal data.

Q 2. How are the various personal and non-personal data associated with the metaverse protected in your jurisdiction?

Under section 2(1) of the PDPA, 'personal data' means data about an individual who can be identified: (1) from that data; or (2) from that data and other information to which the organisation has or is likely to have access.

Examples of data which are likely to be considered personal data include an individual's name, email address and biometric data (such as a facial image, fingerprint or iris print). Electronic identifiers and data that is automatically generated, such as internet protocol (IP) addresses, device fingerprints, user activity or behavioural data may also potentially be considered personal data, depending on the specific circumstances. It is also possible that avatars that closely resemble the real-world appearance of individuals (eg, if generated through the use of photographs of an individual) may be treated as personal data.

Personal data also includes 'derived personal data' which is defined under section 2(1) of the PDPA to mean personal data about an individual which is derived by an organisation in the course of business from other personal data about the individual or another individual, in the possession or under the control of the organisation, but does not include personal data derived by the organisation using certain prescribed means or methods. This is likely to include new data elements created through the processing of personal data, such as through mathematical, logical, statistical, computational, algorithmic or other analytical methods based on the application of business rules.

1 Speech by Deputy Commissioner, Yeong Zee Kin, at NUS Conference 'Understanding the Metaverse: Law, Policy & Practice', 20 September 2022.

Some of the data processed by metaverse platforms may potentially be considered to be sensitive personal data by the PDPC. While the PDPA does not specifically provide for a separate category of 'sensitive personal data', the PDPC has previously meted out higher penalties in respect of breaches of the PDPA involving personal data regarded as 'sensitive' and has issued guidance stating that organisations should take greater care and provide a higher standard of protection to such sensitive personal data.

Examples of sensitive personal data may include financial information, such as credit card numbers, medical information and personal data relating to children.

Q 3. In relation to personal data, what are the data protection principles (eg, transparency) applicable on the metaverse? What are the most common types of infringement of data protection principles in the metaverse (eg, data minimisation) in your jurisdiction?

Organisations collecting, using or disclosing personal data in Singapore will generally need to comply with the nine data protection obligations under the PDPA, which apply equally to interactions in the metaverse as on other digital platforms or in the real world. These obligations are outlined below.

Consent, purpose limitation and notification

Before collecting, using or disclosing personal data in Singapore, an organisation must: (1) notify the individual of the purposes for which it will be collecting, using or disclosing their personal data; and (2) unless certain exceptions apply, obtain the individual's consent for the collection, use or disclosure (as the case may be) of their personal data against notified purposes, which must be purposes that a reasonable person would consider appropriate in the circumstances.

Access

An organisation shall ensure that on an individual's request, it shall, as soon as reasonably possible, provide that individual with: (1) the personal data about the individual that is in the possession or under the control of the organisation; and (2) information about the ways in which that personal data has been or may have been used or disclosed by the organisation within the year before the date of the request.

Correction

Unless an organisation is satisfied on reasonable grounds that a correction should not be made, an organisation shall, on receiving a request from an individual to correct an error or omission in their personal data that is in the possession or under the control of the organisation: (1) correct the personal data as soon as practicable; and (2) send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction was made, unless that other organisation does not need the corrected personal data for any legal or business purpose.

Accuracy

An organisation must make a reasonable effort to ensure that personal data collected by or on its behalf is accurate and complete, if the personal data is likely to be: (1) used to make a decision that affects the individual concerned; or (2) disclosed by the organisation to another organisation.

Protection

An organisation is required to protect personal data in its possession or under its control by making reasonable security arrangements to prevent: (1) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks to the personal data in question; and (2) the loss of any storage medium or device on which personal data is stored.

Retention limitation

An organisation shall cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular customers, as soon as it is reasonable to assume that: (1) the purposes for which the personal data was collected is no longer being served by retention of the personal data; and (2) retention is no longer necessary for legal or business purposes.

Transfer limitation

An organisation must not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA, to ensure that organisations provide a standard of protection in regard to personal data so transferred that is comparable to the protection under the PDPA.

Data breach notification

It is mandatory for organisations to notify the PDPC of a data breach that results in, or is likely to result in, significant harm to individuals to whom any personal data affected by a data breach relates ('affected individuals') or is of a significant scale (ie, if the data breach affects no fewer than 500 individuals). The PDPC has also established a prescribed list of categories of personal data which it regards as meeting the former requirement. Organisations will also generally be required to notify the affected individuals if the data breach is likely to result in significant harm to them, unless an exception applies.

Accountability

An organisation must undertake measures in order to ensure that they meet their obligations under the PDPA and demonstrate that they can do so when required. These measures include developing and implementing: (1) an internal-facing data protection policy setting out the purposes as to how the organisation collects, uses and discloses its employees' personal data; and (2) an external-facing data protection policy setting out the purposes for which the organisation collects, uses and disclosers its customers' personal data. Organisations should also develop a process to receive and respond to complaints arising with respect to the PDPA.

Data portability

One of the key characteristics of the metaverse is interoperability, which often refers to the portability of data and digital assets across metaverse platforms. This may potentially be facilitated in part by the data portability obligation set out in the PDPA, which is due to come into effect at a later date that has yet to be announced.

Under this obligation, on receiving a data portability request from an individual, it is expected that an organisation will be required to transmit the individual's personal data that is in the organisation's possession or under its control, to another organisation designated by the individual, in a commonly-used machine-readable format. The data portability obligations are intended to apply to applicable data that is the subject of a data portability request regardless of whether the data is stored or processed in, or transmitted from, Singapore or a foreign country or territory.

That said, as currently drafted, the data portability obligation appears to be primarily targeted at portability on a 'one-off' basis instead of on an ongoing basis. This may not be entirely suitable for many metaverse use cases which are likely to require frequent data exchanges on an ongoing basis.

Sanctions

The PDPC is empowered under the PDPA to take enforcement action in respect of breaches of the data protection obligations under the PDPA, including by issuing mandatory directions or imposing financial penalties of up to SGD1m (approximately US$765,000) or ten per cent of the relevant organisation's annual turnover in Singapore, whichever is greater (PDPA, sub-sections 48I, 48J).

In addition, individuals who suffer loss or damage directly as a result of a contravention by an organisation of the data protection obligations have a right of action for relief which may be pursued through civil proceedings in court. The court may grant a successful claimant all or any of the following: relief by way of an injunction or declaration; damages; and/or any other relief as the court thinks fit (section 48O).

The PDPA also provides for various criminal offences relating to the mishandling of personal data, such as relating to: the unauthorised disclosure of personal data (section 48D); improper use of personal data (section 48E); unauthorised re-identification of anonymised information (s 48F); and making unauthorised access or correction requests (section 51).

Q 4. Are there any policies, strategies or regulations in your jurisdiction focused on ensuring protection of minors' data? What is the age of consent for data protection purposes? Is it necessary to verify the consent provided by a responsible adult?

Although the PDPC has yet to issue guidelines specifically addressing personal data processing in the metaverse, it has recently published guidance relating to the processing of children's personal data in the digital environment which may be particularly relevant to metaverse platforms and applications with a young user base.

The PDPC has taken the position that a child between 13 and 17 years of age is generally capable of giving valid consent to the collection, use and/or disclosure of their personal data and withdrawing their consent to the same, provided that the external-facing policies applicable to such collection, use and disclosure are readily understandable by such a child.[2] Nonetheless, if an organisation has reason to believe that the child does not have sufficient understanding of the nature and consequences of giving such consent, the organisation should obtain consent from the child's parent or guardian.

The PDPC also recommends that organisations take the following measures to comply with the data protection obligations under the PDPA in respect of children's personal data:

- when communicating with children, organisations should use language that is readily understandable by them;
- organisations should adopt data minimisation policies to limit the collection and sharing of children's personal data. For example, account information of children should not be made public and searchable by default; and
- organisations must not collect, use or disclose personal data of individuals for purposes that a reasonable person would not consider appropriate in the circumstances, such as purposes that are in violation of the law or which would be harmful to the individual concerned, or to target harmful or inappropriate content (as defined in the Code of Practice for Online Safety issued by the Infocomm Media Development Authority of Singapore (IMDA)) at a child.

As the ability to determine or monitor the precise location of a child may give rise to a risk of misuse that may compromise the child's safety, organisations should adopt a data minimisation approach and implement relevant safeguards, such as by disabling geolocation functionality by default so that precise location data is not automatically collected when the relevant product or service is first used.

Q 5. How are international data transfers regulated in your jurisdiction? Is there any case law or are there any decisions by a regulator regarding infringements of these rules in your jurisdiction?

The metaverse is often described as offering a borderless experience, allowing people to live, work, play and interact with each other seamlessly across the globe. Such an experience is likely to have to be supported by cross-border data transfers, possibly at tremendous scale, which will involve the sharing of personal data across servers located in multiple jurisdictions.

When an organisation transfers personal data out of Singapore (such as where the organisation transmits personal data to an overseas vendor or stores personal data in an overseas data centre), the organisation must comply with the Transfer Limitation Obligation. In practice, the most common way to comply with this obligation is to enter into a data transfer agreement with the overseas recipient that: (1) requires the recipient to provide in regard to the personal data transferred

2 PDPC, *Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment* (2024).

to the recipient a standard of protection that is at least comparable to the protection under the PDPA; and (2) specifies the countries and territories to which the personal data may be transferred under the contract.

A metaverse platform or service provider seeking to transfer personal data across various jurisdictions in Southeast Asia may wish to consider using the ASEAN Model Contractual Clauses, which are model data protection clauses for data transfers which are recognised as fulfilling data protection requirements relating to the transfer of personal data by regulators in various ASEAN (Association of Southeast Asian Nations) jurisdictions, including the PDPC in Singapore.[3] Singapore also recognises the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors System (PRP) certifications for overseas transfers of personal data under the PDPA.

3 PDPC, *Guidance for Use of ASEAN Model Contractual Clauses for Cross Border Data Flows in Singapore* (2021).

AI on the metaverse

Lam Chung Nian *WongPartnership, Singapore*
Huey Lee *WongPartnership, Singapore*

The Singaporean government has generally taken a balanced approach towards artificial intelligence (AI) governance, seeking to balance safeguards with the need to maintain opportunities for AI technologies to develop. Although there is currently no legislation specifically regulating the use of AI in the metaverse, the government has published various guidelines, principles, and testing and verification frameworks in consultation with sector players, of which organisations using and developing AI systems should be aware.

Q 1. Are there any policies, strategies or regulations applicable to AI or the use of AI on the metaverse in your jurisdiction?

Use of personal data

Where a metaverse platform collects, uses or discloses personal data in connection with AI-powered functionality, such as for the purposes of automated decision-making or generating personalised recommendations, it should ensure that it complies with the applicable data protection obligations (see the chapter on data for more information). In particular:

Consent, notification and purpose limitation obligations

Organisations may generally collect, use or disclose personal data about an individual only for purposes: that a reasonable person would consider appropriate in the circumstances; and that the individual has been informed about the organisation.

The Personal Data Protection Act 2012 (PDPA) states that the intention underlying the consent and notification obligations is to enable individuals to provide meaningful consent and organisations should craft notifications accordingly so as to enable individuals to understand how their personal data will be processed to achieve the stated purpose. Notifications should be proportionate to the risks of the relevant use case, for example, taking into account the potential harm to the individual and the level of autonomy of the AI system.

Accuracy obligation

If personal data is likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates, the organisation is required to ensure that the personal data is reasonably correct and complete, so as to ensure that the decision is made taking into account all relevant personal data.

Accountability obligation

Organisations that use AI systems should be transparent and include in their written policies information on the relevant practices and safeguards to achieve fairness and reasonableness. The level of detail to be provided should be proportionate to the risks in each use case, for example, taking into account potential harm to the individual and the level of autonomy of the AI system. Organisations must make information about such policies and practices available to individuals on request.

The PDPC has also recommended that organisations include additional information in their external-facing written policies to build consumer trust and confidence, such as: (1) behind-the-scenes measures taken to ensure that personal data is used in a safe and trusted manner within the AI system; and (2) data quality and governance measures taken during the operation of the AI system, insofar as such information is relevant and providing such information does not compromise security, safety or commercial confidentiality.[4]

4 PDPC, *Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems* (2024).

AI Verify and Model AI Governance Framework

In 2023, the AI Verify Foundation (the 'Foundation') was launched, with the goal of boosting AI testing capabilities in Singapore and assisting organisations with objectively demonstrating responsible use of AI through standardised tests. The Foundation works in collaboration with industry players and the open-source community to develop AI testing frameworks, standards and best practices, and create a neutral platform for open collaboration and ideation for the testing and governance of AI.

The Foundation will support the further development and use of AI Verify, which refers to an AI governance testing framework and associated software toolkit that was initially developed by the Infocomm Media Development Authority (IMDA) in consultation with industry players.

The AI Verify testing framework builds on internationally recognised AI governance principles, guidelines and frameworks, including the Singapore Model AI Governance Framework published by the PDPC, as well as those published by international bodies such as the Organisation for Economic Co-operation and Development's AI Principles and the United States National Institute of Standards and Technology's AI Risk Management Framework.

The Framework currently consists of the following 11 principles organised in the following five categories:

Categories	Principles
Transparency on the use of AI and AI systems	• transparency
Understanding how AI models reach decisions	• explainability • repeatability/reproducibility
Safety and resilience of AI systems	• safety • security • robustness
Fairness/no unintended discrimination	• fairness • data governance
Management and oversight of AI systems	• accountability • human agency and oversight • inclusive growth, societal and environmental wellbeing

The associated software toolkit is an open source, extensible toolkit which can be used to assess AI systems against the principles set out in the Framework. According to the AI Verify Foundation, the toolkit can be used out of the box with supervised learning AI models, including binary classification, multiclass classification and regression models. The AI Verify Foundation has invited third-party developers and researchers to contribute to the toolkit by developing third-party plug-ins and/or designing customised reports.

Generative AI

In 2024, the AI Verify Foundation and the IMDA jointly published a draft Model AI governance framework for generative AI (the 'GenAI Framework'), which built on the existing AI Verify governance framework. The GenAI Framework acknowledges the transformative potential of generative AI and aims to establish global principles for a trusted AI environment, addressing emerging issues and incorporating insights from discussions, technical work and ongoing evaluations.

The GenAI Framework seeks to balance fostering innovation with user protection by outlining nine key dimensions for governance and by drawing out various issues that should be considered when creating a trusted ecosystem for generative AI to address concerns without stifling innovation.

Organisations using AI in the metaverse should be aware of these AI governance frameworks, including the associated principles and guidelines, and should take advantage of the associated testing and verification software toolkit where appropriate, so as to demonstrate responsible use of AI.

Human rights, accessibility and digital ethics

Lam Chung Nian *WongPartnership, Singapore*
Huey Lee *WongPartnership, Singapore*

Q 1. Are there any human rights, accessibility and digital ethics strategies, polices or regulations applicable to the metaverse in your jurisdiction?

Singapore has put in place various regulatory frameworks to address online misinformation, content moderation, online scams and other harmful online conduct which may be relevant to the metaverse.

Broadcasting regime

A metaverse platform or application which provides digital content through the internet in or from Singapore is likely to be automatically class-licensed under the Broadcasting Act 1999 of Singapore as an internet content provider (ICP).

Such class licensees are required to comply with various class licence conditions, ensuring that its service complies with codes of practice such as those that the Infocomm Media Development Authority of Singapore (IMDA) issues, including, for example, the Internet code of practice which provides (among other things) that ICPs must strive to ensure that 'prohibited material' is not broadcast via the internet to users in Singapore. This refers to material that is objectionable on the grounds of public interest, public morality, public order, public security, national harmony or is otherwise banned by applicable Singaporean laws.

Licensees must also remove or ban the broadcast (in whole or in part) of a programme (which may include certain digital content) included in its service if: IMDA informs the licensees that the broadcast of the whole or part of the programme is contrary to a Code of Practice applicable to the licensee; or the programme is contrary to public interest, public order or national harmony, or is offensive in terms of good taste and honesty.

The Broadcasting Act was recently updated to provide the IMDA with additional powers to promote online safety in Singapore through various measures targeted at 'egregious content' on online communication services (OCS). Such content includes, for example, that which advocates or instructs on suicide or self-harm, child pornography or content that advocates or instructs on terrorism (among other things). A metaverse platform or service which has the characteristics of a social media service may potentially be considered to be an OCS.

The IMDA's powers can be broadly categorised as follows:

Proactive

The IMDA may designate an OCS with a Singapore end-user link as a 'regulated OCS'. Such companies must comply with the applicable codes of practices published by the IMDA, such as the Code of Practice for Online Safety.

Reactive

The IMDA may also issue directions to OCS providers (including non-regulated OCS providers) requiring them to take action in connection with egregious content, such as requiring such providers to cut access to egregious content for users in Singapore.

Online criminal harms

The Online Criminal Harms Act 2023 of Singapore (OCHA) recently came into effect. The Act was introduced to enable the Singaporean government to deal with online activities which are criminal in nature, such as online scams.

The OCHA empowers designated officers to issue various directions to any online service provider (which may potentially include a metaverse platform or application) to restrict the exposure of Singaporean users to criminal activities on the relevant online service, such as by requiring the provider to stop communicating specified online content, prohibit access from Singapore to specified content or restrict interaction in relation to a specified account on their service.

These directions can be issued where there is reasonable suspicion that an online activity is involved in the continuation of the commission of a specified offence. For scams and malicious cyber activities, the threshold for issuing directions is lower: directions can be issued when there is suspicion or reason to believe that any online activity is being carried out in preparation for or in furtherance of the commission of a scam or a malicious cyber-enabled offence.

The Singapore Ministry of Home Affairs has indicated that it intends to issue codes of practice and directives to strengthen its partnership with providers of online services to counter scams and malicious cyber activities, including a code of practice for app distribution services (eg, app stores), which may require providers of such services to put in place systems and processes to mitigate users' exposure to harmful apps.

Q 2. Considering the risks of misinformation and the risks associated with fake news and deep fakes on the metaverse, are there any strategies, policies or regulations in your jurisdiction aiming to mitigate them/promote freedom of expression and non-censorship?

Under the Protection from Online Falsehoods and Manipulation Act 2019 (POFMA), where a false statement of fact has been or is being communicated in Singapore through the internet, the Singaporean government may issue a range of directions to electronic platforms carrying such false statements. Such directions may (among other things) require the platform to carry a 'correction notice' alongside the relevant statements and/or to stop communicating the statements, provided it is in the 'public interest' to issue such directions.

Although there has yet to be a POFMA notice issued in respect of a falsehood in the metaverse, POFMA orders have previously been issued in respect of webpages and blog posts, as well as in relation to Facebook posts, Instagram stories, X (formerly known as Twitter) posts, YouTube videos and forum posts.

POFMA also provides for various criminal offences relating to misinformation, such as in relation to communication of false statements of fact that are prejudicial to public health, safety, tranquillity or finances, among other matters (section 7), making or altering bots for communication of false statements of fact (section 8) and providing services for communication of false statements of fact (section 9).

Singapore also has a Protection from Harassment Act 2014 (POHA) which protects persons against harassment, unlawful stalking and false statements of fact, including such actions carried out via social media and other electronic platforms. The POHA defines criminal offences for, among other things, harassment, causing alarm or distress, causing fear, the provocation or facilitation of violence, unlawful stalking, etc, and also allows for protection orders to be issued against the perpetrators of such acts.

Intellectual property

Lam Chung Nian *WongPartnership, Singapore*
Huey Lee *WongPartnership, Singapore*

Q 1. What are the public policies, strategies or regulations relating to intellectual property which are applicable to the metaverse in your jurisdiction?

In the metaverse, users are able to view, explore and interact with digital assets, including digital avatars, virtual buildings and landscapes, digital 'twins' of real-world items and structures, among many others. Such digital assets may be protected by one or more intellectual property (IP) right under Singaporean law.

The Intellectual Property Office of Singapore (IPOS) administers the IP legislative framework in Singapore, which includes copyrights, trademarks, designs and patents.

Copyright

Under the Copyright Act 2021 of Singapore, creators of protected works (including works in electronic form) may enjoy various exclusive rights, such as the rights of reproduction and/or communication to the public, so long as the requirements for copyright subsistence and protection are met. The exclusive right of reproduction may extend in some cases to reproduction of a two-dimensional artistic work in three-dimensional form and vice versa, as well as to the conversion of an authorial work into a digital or electronic machine-readable form.

Trademarks

Singapore operates a system in respect of registered trademarks under the Trademarks Act 1998 of Singapore, and the registered proprietor is granted a statutory monopoly over use (and authorisation of use) of the trademark in Singapore in relation to the goods and/or services for which it is registered for the duration of the registration, subject to certain exceptions. IPOS has issued guidelines on the registration of trade marks in relation to non-fungible tokens (NFTs), virtual goods, and metaverse-related goods and services, which among other things, clarifies acceptable specifications for such trademarks.

Designs

The Registered Designs Act 2000 of Singapore protects registered designs in Singapore, provided that the design qualifies as a design, is a new design and does not fall within certain excluded categories. The Act specifically recognises that designs in respect of non-physical products (such as intangible objects) may be registered, provided the relevant requirements are met.

Patents

The Patents Act 1994 of Singapore confers protection on patentable inventions in Singapore, including potentially software-implemented inventions and computer programs, provided that the invention satisfies the requirements of novelty, inventive step and industrial applicability as prescribed under the Act. Patents are generally valid for 20 years from the date of filing, subject to the payment of annual renewal fees in compliance with the prescribed procedures.

Digital transactions and ownership

Lam Chung Nian *WongPartnership, Singapore*
Huey Lee *WongPartnership, Singapore*

Q 1. Are there any relevant policies, strategies or regulations applicable to tokens, non-fungible tokens (NFTs) and digital assets on the metaverse in your jurisdiction?

Singapore users have also been among the first to embrace metaverse interactions. It has been asserted that the first wedding on the decentralised virtual world 'The Sandbox' was held in 2022 between Singaporeans, though there was also a physical wedding.[5] Various Singaporean banks have acquired plots of virtual land in the metaverse to engage with consumers in immersive virtual worlds.[6]

Organisations operating in the metaverse will be pleased to know that Singaporean law has generally taken a facilitative approach towards the recognition and protection of digital transactions and assets.

The Electronic Transactions Act 2012 of Singapore (ETA) takes a technology neutral approach and specifically provides that electronic records are not to be denied legal effect, validity or enforceability solely on the grounds that they are electronic in nature.[7] The ETA also recognises the validity of electronic signatures provided that the signor is sufficiently identified and the signature method is sufficiently reliable.[8] In addition, the ETA also implements the UNCITRAL Model Law on Electronic Transferable Records which was adopted by the UN Commission on International Trade Law (UNCITRAL) in 2017 and facilitates the use of transferable documents and instruments (such as bills of lading, promissory notes and cheques) in electronic form.

Q 2. How is property defined on the metaverse? Are there any relevant policies, strategies or regulations applicable to the ownership of digital assets on the metaverse in your jurisdiction?

Although there is no legislation in Singapore specifically dealing with property on the metaverse, the High Court of Singapore has previously held that digital assets, such as Bitcoin and non-fungible tokens (NFTs), appear to fulfil the criteria set out in the landmark English case of *National Provincial Bank v Ainsworth*.[9] Under Singaporean law, such assets are therefore in principle capable of being the subject of proprietary right and, accordingly, can be the subject of a trust,[10] or of injunctive or equitable relief.[11] Accordingly, a metaverse user may, depending on the implementation mechanics, potentially be able to enforce their ownership of digital assets in the metaverse under Singapore law, although the success of such an action will ultimately depend on the specific circumstances.

When considering the ownership of digital assets (on the metaverse or otherwise), there are generally two distinct layers to be considered: (1) ownership of the intellectual property (IP) rights in the digital asset (see the chapter on intellectual property); and (2) ownership of the proprietary right in the digital asset, assuming that such right exists.

5 Darrelle Ng, 'Couples say "I do" in Singapore's first metaverse wedding', *Channel News Asia*, 23 September 2022.
6 Prisca Ang, 'DBS enters metaverse in tie-up with The Sandbox to create virtual BetterWorld', *The Straits Times*, 10 September 2022; Cheow Sue-Ann, 'OCBC steps into metaverse, first Singapore bank to offer virtual banking experience', *The Straits Times*, 5 April 2023.
7 ETA, ss 6, 16E.
8 ETA, s 8.
9 [1965] UKHL 1.
10 *Bybit Fintech Ltd v Ho Kai Xin* [2023] SGHC 199.
11 *CLM v CLN* [2022] SGHC 46; *Janesh s/o Rajkumar* [2022] SGHC 264.

In the context of metaverse platforms and services, the surrounding contractual arrangements are likely to be relevant in determining ownership. For example, platform terms and conditions that provide that the platform reserves ultimate control over a digital asset and is entitled to remove it from a user's account at any time, may render it more likely that the digital asset will be found to be owned by the platform rather than the user.[12] Ultimately, however, the final analysis is likely to be quite fact dependent and require a close examination of all the surrounding circumstances.

12 *Lee Kien Meng v Cintamani Frank* [2015] SGHC 109.