Chambers AND PARTNERS

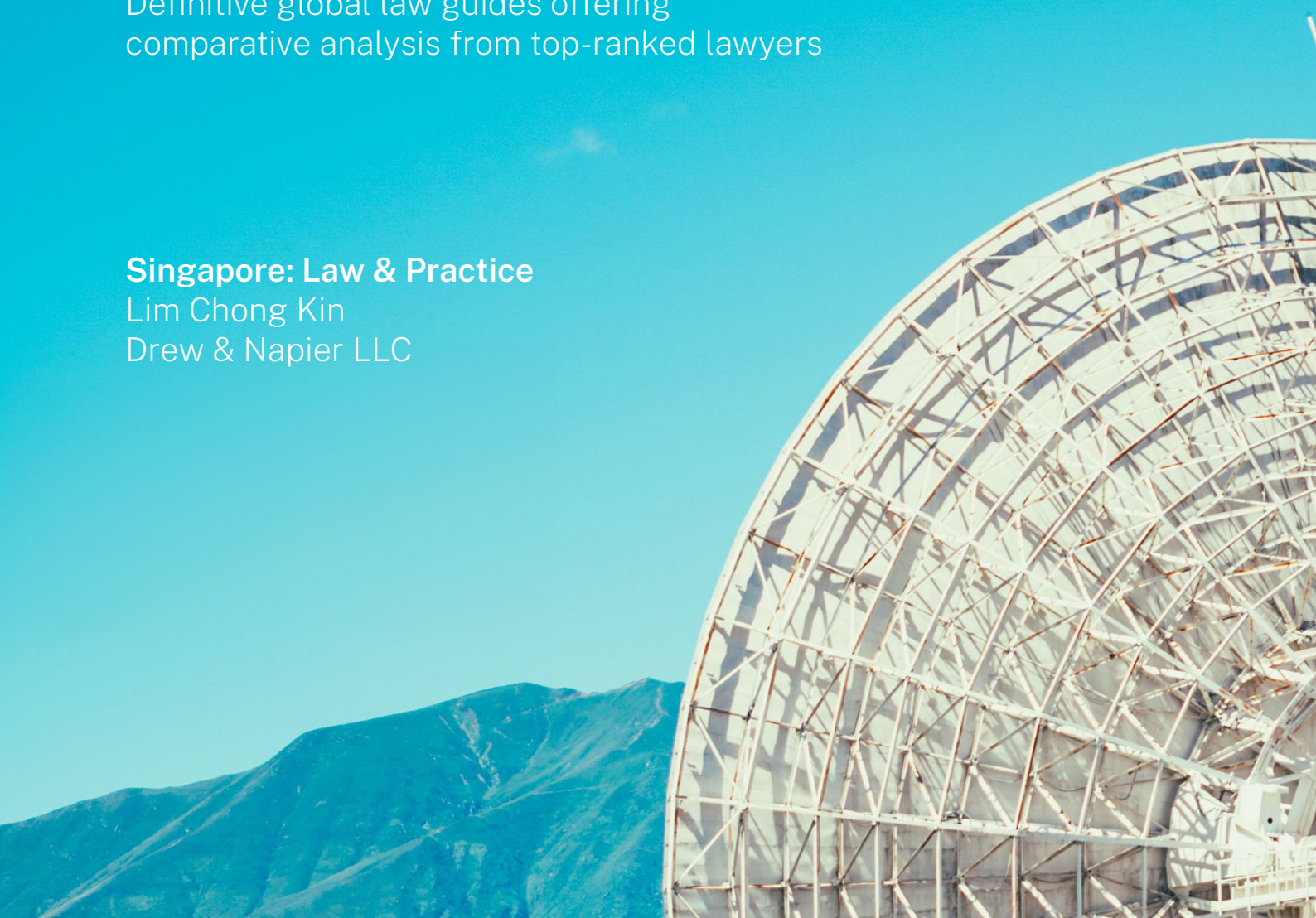
CHAMBERS GLOBAL PRACTICE GUIDES

TMT 2026

Definitive global law guides offering comparative analysis from top-ranked lawyers

Singapore: Law & Practice

Lim Chong Kin
Drew & Napier LLC



SINGAPORE

Law and Practice

Contributed by:
Lim Chong Kin
Drew & Napier LLC

Contents

1. Digital Economy p.4
1.1 Legal Framework p.4
1.2 Key Challenges p.5
1.3 Digital Economy Taxation p.5
1.4 Taxation of Digital Advertising p.5
1.5 Consumer Protection p.6
1.6 The Role of Blockchain in the Digital Economy p.6

2. Cloud and Edge Computing p.7
2.1 Highly Regulated Industries and Data Protection p.7

3. Artificial Intelligence p.9
3.1 Liability, Data Protection, IP and Fundamental Rights p.9

4. Internet of Things p.11
4.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.11
4.2 Compliance and Governance p.12
4.3 Data Sharing p.12

5. Audiovisual Media Services p.13
5.1 Requirements and Authorisation Procedures p.13

6. Telecommunications p.14
6.1 Scope of Regulation and Pre-Marketing Requirements p.14
6.2 Net Neutrality Regulations p.16
6.3 Emerging Technologies p.16

7. Challenges With Technology Agreements p.16
7.1 Legal Framework Challenges p.16
7.2 Service Agreements and Interconnection Agreements p.17

8. Trust Services and Digital Entities p.18
8.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.18

9. Gaming Industry p.19
9.1 Regulations p.19
9.2 Regulatory Bodies p.20
9.3 Intellectual Property p.20

10. Social Media p.21
10.1 Laws and Regulations for Social Media p.21
10.2 Regulatory and Compliance Issues p.22

11. Data Privacy and Cybersecurity p.23
11.1 Data Privacy in Telecommunications p.23
11.2 Cybersecurity in Digital Media and Streaming Services p.23

Drew & Napier LLC has a highly regarded TMT practice group, consistently ranked as the leading IT, telecommunications, broadcasting and multimedia legal practice in Singapore. The firm possesses unparalleled transactional, licensing and regulatory experience in the areas of telecommunications, technology, media, data protection and cybersecurity. Its data protection, privacy and cybersecurity practice group has been at the forefront of data protection law in Singapore since 2013, and has worked on significant data protection enforcement cases and appeals, including cases with cybersecurity elements. The firm established the Drew Data Protection & Cybersecurity Academy in 2020 to offer additional services related to data protection and cybersecurity compliance, including training, data protection consulting and external Data Protection Officer services. Drew & Napier is the preferred counsel of many regional companies, multinationals, associations, government bodies and industry regulators, which it regularly assists on a wide range of matters in Singapore and ASEAN member countries.

Author

Lim Chong Kin heads Drew & Napier's highly regarded TMT practice group. His clients include telecoms and media regulators, global carriers, technology market leaders, global broadcasters and content providers. Chong Kin has worked on every significant development in the Singapore TMT market, and continues to play a key role in the development of sectoral competition regulation in Singapore. He was the lead external counsel in the liberalisation of the telecommunications, media and postal sectors, and has assisted regulators in conceptualising and drafting "first-of-its-kind" sectoral competition legislation and frameworks.

Drew & Napier LLC

10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

Tel: +65 6535 0733
Fax: +65 6535 4906
Email: mail@drewnapier.com
Web: www.drewnapier.com

1. Digital Economy

1.1 Legal Framework

The following chapter featured in TMT 2025 and is awaiting update from the firm.

A patchwork of legislation is currently available to regulate the digital economy in Singapore, including in relation to consumer protection, the sale of goods and services, payment services and personal data protection.

Digital Payment Solutions

Under the Payment Services Act 2019 (PSA), providers of digital payment solutions (such as e-wallet services) may need to apply for either an either a standard payment institution (SPI) licence or a major payment institution (MPI) licence if they offer the following services:

- account issuance services that involve issuing a payment account, or any service relating to any operation required for operating a payment account;
- domestic money transfer services that involve providing a local fund transfer service;
- merchant acquisition services that involve accepting and processing payment transactions and payment receipts for and on behalf of a merchant;
- e-money issuance services that involve the issuance of e-money for persons to make payment transactions;
- cross-border money transfer services that involve providing inbound or outbound remittance services in Singapore or arranging remittance from one country or territory to another; or
- digital payment tokens (DPT) services, on a non-exhaustive basis, that involve buying or selling virtual currency, or providing a platform to allow persons to exchange virtual currency in Singapore.

The PSA also imposes a stock and flow cap on personal payment accounts issued by MPI licensees, to protect customers by limiting potential loss from the customer's account. Personal payment accounts issued by an MPI are subject to a load capacity (ie, the maximum amount of funds that can be held at any given time) of SGD20,000 and an annual transaction flow cap (ie, the maximum total outflow over a rolling 12-month period) of SGD100,000.

E-Commerce

E-marketplaces and e-retailers should ensure that they conform with the Consumer Protection (Fair Trading) Act 2003 (CPFTA), which applies where the consumer or supplier is resident in Singapore or where the offer or acceptance relating to the consumer transaction is made in or sent from Singapore. Therefore, in the digital economy where cross-border transactions are the norm, the CPFTA will apply where this nexus to Singapore is established.

The CPFTA accords customers rights and prohibits sellers from engaging in unfair practices or selling defective goods. If a supplier engages in unfair practices such as making false representations, deceiving consumers or taking advantage of consumers in certain circumstances, the consumer may take legal action against them under the CPFTA. In addition, where a good does not conform to the agreement between the parties, the consumer has a right against the supplier to demand repair or replacement of the good at the supplier's expense or, alternatively, a price reduction or refund.

Moreover, in June 2020 the first national standard for e-commerce transactions, Technical Reference 76 (TR 76), was issued by Enterprise Singapore and the Singapore Standards Council. TR 76 serves as a practical reference for e-retailers and online intermediaries to build trust and transparency in online transactions. It was revised in 2022 to include additional anti-scam guidelines for e-retailers and e-commerce marketplaces to offer better protection for consumers transacting online.

The Competition and Consumer Commission of Singapore (CCCS) has also updated its guidelines in relation to digital markets. For instance, the CCCS Guidelines on Market Definition have clarified issues relating to market definition, which are particularly relevant in digital markets that feature multi-sided platforms. Notably, the CCCS has defined a "multi-sided platform" as an undertaking acting as a platform that facilitates interactions between two or more groups of users and creates value for sellers or buyers on one

side of the platform by matching or connecting them with buyers or sellers on the other side of the platform.

The Personal Data Protection Act (PDPA) strikes a balance between consumers' commercial needs and safeguarding their personal data. Notably, while organisations are required to obtain the consent of individuals to collect, use or disclose personal data, the PDPA provides for exemptions to the consent obligation, which may be useful to e-commerce providers. For example, the business improvement exception under the PDPA allows organisations to use personal data, without consent, for the purposes of:

- improving any goods or services provided;
- improving methods or processes for the operations of the organisation;
- learning the behaviour and preferences of the individual or another related individual in relation to the goods or services provided by the organisation; and
- identifying any goods or services provided by the organisation that may be suitable for the individual or another individual.

1.2 Key Challenges

No content provided in this jurisdiction.

1.3 Digital Economy Taxation

Goods and Services Tax (GST) is imposed on the supply of digital services and goods in Singapore. The Goods and Services Tax Act (GST Act) governs the imposition and collection of GST in Singapore.

Digital services are defined as any services supplied over the internet or other electronic network, the nature of which renders its supply essentially automated with minimal or no human intervention, and impossible without the use of information technology. GST is payable by the consumer upon the purchase of digital services from GST-registered overseas service providers. Only digital services provided by GST-registered service providers are subject to GST.

A mandatory registration regime exists for overseas digital service providers who have an annual global turnover of more than SGD1 million and sell more than SGD100,000 worth of digital services to customers in Singapore over a 12-month period.

Since 1 January 2023, GST also applies to all remote services (ie, digital and non-digital services) purchased by consumers in Singapore from GST-registered overseas service providers. Examples of such remote services include:

- downloadable digital content;
- subscription-based media;
- software programs;
- electronic data management services;
- support services performed via electronic means to arrange or facilitate transactions, which may not be digital in nature;
- professional services;
- personal services; and
- educational, professional membership and examination services.

For physical goods supplied over the internet, as long as the goods are delivered locally, the supply of the goods should be standard-rated and GST should be charged to the consumer.

1.4 Taxation of Digital Advertising

The provision of web-advertising services is considered as a form of media sales in Singapore. Media sales include the sale of media space for online advertising, in various forms, such as page view, impression, hit rate, electronic data mail and SMS messages, in digital media via email, internet and mobile phone. As with any supply of service made in Singapore, web-advertising services attract GST unless they qualify for zero-rating relief as an international service under the GST Act.

With effect from 1 Jan 2022, the supply of media sales will be zero-rated (ie, GST is charged at 0%) if the supply is contractually made to an overseas person and directly benefits an overseas person and/or a GST-registered person belonging in Singapore. Such a person (contractual client) will generally be regarded by the Comptroller as the "sole direct beneficiary" if:

- the service agreement between the provider of the services and the contractual client does not specify

or require the services to be provided to another person; and
- the provider of the services only liaises with and is accountable to the contractual client for the service deliverables.

1.5 Consumer Protection

The consumer protection law in Singapore that applies to digital goods and services is the CPFTA – see **1.1 Legal Framework** (E-Commerce).

1.6 The Role of Blockchain in the Digital Economy

Two types of digital assets are likely to play prominent roles in the digital economy: cryptocurrencies and non-fungible tokens (NFTs), which may be regulated by the Monetary Authority of Singapore (MAS) under the PSA or the Securities and Futures Act 2001 (SFA).

Under the SFA, the offer or issue of digital assets such as cryptocurrencies or NFTs may be regulated if they constitute capital market products under Section 2 (1). Capital markets products include any securities, derivatives contracts and contracts or arrangements for purposes of leveraged foreign exchange trading. Digital assets that fall within the scope of digital payment tokens (DPTs) are subject to the regulatory regime under the PSA, which defines a DPT as any digital representation of value that:

- is expressed as a unit;
- is not denominated in any currency, and is not pegged by its issuer to any currency;
- can be transferred, stored or traded electronically;
- is, or is intended to be, a medium of exchange accepted by the public, or a section of the public, as payment for goods or services or for the discharge of a debt; and
- satisfies such other characteristics as the MAS may prescribe.

Subject to applicable exemptions provided for therein, the PSA requires a person who carries on a business of providing a DPT service as defined under Part 3 of the First Schedule to the PSA to apply for either a standard payment institution (SPI) licence or a major payment institution (MPI) licence.

On top of compliance with the PSA, licence holders must comply with the MAS's guidelines and notices, such as the Guidelines on Provision of Digital Payment Token Services to the Public and the Guidelines on Consumer Protection Measures by DPT Service Providers, revised on 19 September 2024.

In addition, all holders of a payment services licence under the PSA that carry on a business of providing DPT services (DPT Licensees) are required to comply with cyber hygiene requirements set out in the MAS Notice on Cyber Hygiene and the MAS Technology Risk Management Guidelines, which require financial institutions generally to establish sound and robust technology risk governance and maintain cyber resilience. MAS Notice PSN05 on Technology Risk Management was also recently extended to DPT Licensees, to improve information technology resilience and maintain trust and confidence in DPT services.

NFT trading is likely to become more commonplace and a part of transacting in the virtual space. While there is no legislation that specifically targets NFTs, issues such as ownership continue to be governed by the principles of intellectual property and contract law. A contract for the purchase of NFTs usually contains three distinct subject matters that are capable of ownership by different people:

- the first is the code on the blockchain, which may identify and authenticate the asset;
- the second is the asset itself; and
- the third is the intellectual property rights in respect of the asset.

The relevant intellectual property right is usually copyright, as most NFTs constitute a form of artistic expression that is afforded protection under the Copyright Act 2021 (CA). Therefore, contracts may include the assignment of copyright or a licence. Assignments of copyright must comply with the formalities stipulated in the CA and must be in writing and signed by or on behalf of the assignor. However, this requirement can easily be met even in the virtual space through the application of the Electronic Transactions Act 2010 (ETA). See **8.1 Trust Services and Electronic Signatures/Digital Identity Schemes** for more details on the ETA.

In 2022, the Singapore High Court held that the NFTs being considered in a case satisfied the legal criteria to be considered as property and could be subject to proprietary injunctions. With the growing prominence of NFTs, courts and legislation can be expected to explore and address complex and novel legal issues raised by NFTs in the upcoming years.

2. Cloud and Edge Computing

2.1 Highly Regulated Industries and Data Protection

Limitations are placed on organisations that seek to entrust certain processes or data to the cloud, although most of these limitations are in the context of personal data protection.

Applicable Laws and Guidelines

The main legislation governing the protection of personal data is the PDPA, which defines "personal data" as data, whether true or not, about an individual who can be identified either from that data, or from that data and other information to which the organisation has or is likely to have access. The PDPA is administered and enforced by the Personal Data Protection Commission (PDPC).

There are cross-border data transfer restrictions in the PDPA. Under Section 26, an organisation must not transfer any personal data to a country or territory outside Singapore, except in accordance with prescribed requirements to ensure that the transferred personal data will be accorded a standard of protection that is comparable to that given under the PDPA (the transfer limitation obligation).

The prescribed requirements, as set out in the Personal Data Protection Regulations 2021 (PDPR), require the transferring organisation to ensure that the recipient of the personal data is bound by legally enforceable obligations. These "legally enforceable obligations" include:

- any laws in the jurisdiction to which the personal data is transferred;
- contracts;
- binding corporate rules (BCRs); and
- any other legally binding instrument.

BCRs may be used for recipients that are "related" to the transferring organisation (eg, a parent company or subsidiary), whilst contracts may be used for data transfers to any party. In particular, BCRs and contracts must specify the countries and territories to which the personal data will be transferred under said BCRs or contract.

In addition, under the PDPR, an overseas recipient of personal data is taken to be bound by legally enforceable obligations to provide comparable protection for the transferred personal data if it holds an Asia Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) System or Privacy Recognition for Processors (PRP) System certification (which is granted or recognised under the laws of the country or territory to which the personal data is transferred). That said, transferring organisations that are seeking to rely on this transfer mechanism should ensure that they carry out the necessary due diligence to determine that the overseas recipient is indeed CBPR or PRP-certified under the laws of the country or territory in question.

Furthermore, the PDPC has published a chapter on cloud services in its non-legally binding Advisory Guidelines on the PDPA for Selected Topics, which clarify the application of the PDPA in respect of cloud services (the "Cloud Services Guidelines"). Specifically, an organisation should ensure that the cloud service providers (CSPs) that it engages only transfer personal data in accordance with the PDPA – namely, to locations with comparable data protection regimes – or otherwise have legally enforceable obligations to ensure a comparable standard of protection for the transferred personal data.

On 7 May 2024, the Cybersecurity (Amendment) Bill was passed in Parliament. The amendments have yet to come into force (as of 1 January 2025), but when they do the scope of the Cybersecurity Act 2018 will be expanded to regulate designated providers of cloud computing service. Cloud computing service is defined as a service delivered from a computer or computer system in Singapore or outside Singapore, that enables on-demand administration and broad remote access to a scalable and elastic pool of

shareable computing resources, including where such resources are distributed across several locations.

When the amendments come into force, such designated cloud computing service providers will have to, amongst others, provide cybersecurity information on the service to the Commissioner of Cybersecurity, comply with codes of practice, standards of performance or written directions, and notify the Commissioner of Cybersecurity of any prescribed cybersecurity incident.

Industry Standards and Codes of Conduct

The Multi-Tier Cloud Security (MTCS) Singapore Standard (SS584) is the primary local industry standard for determining the level of cloud security provided by CSPs. The MTCS has three levels of security, with Level 1 being the base standard and Level 3 being the most stringent standard. The adoption of the MTCS is voluntary for CSPs, unless they are participating in bulk tenders for government procurement of public cloud services.

Under the PDPC's Cloud Services Guidelines, MTCS Level 3 certification could give organisations assurance of the CSP's ability to comply with the protection obligation under the PDPA.

The PDPC has also published the 2018 Guidelines for Cloud Outage Incident Response (COIR) (TR 62:2018). Under the voluntary COIR framework, cloud service customers (CSCs) can choose appropriate outage protection measures that would complement their business continuity/discovery recovery capabilities through a set of guidelines that assist CSCs in identifying, evaluating and negotiating protection needs with CSPs to incorporate into their service-level agreements, and the sharing of COIR practices by CSPs through the same set of common parameters. While the adoption of the COIR guidelines is voluntary, CSPs are encouraged to self-disclose their service support capabilities with respect to service outages.

Sector-Specific Regulation

Apart from the PDPA and the Cloud Services Guidelines, the use of CSPs in the financial sector is subject to additional regulation by the sectoral regulator (the MAS). In this respect, the MAS has published the following guidelines for financial institutions (FIs), setting out its position on cloud computing and cloud outsourcing arrangements:

- Technology Risk Management Guidelines;
- ABS (Association of Banks in Singapore) Cloud Computing Implementation Guide 3.0;
- Guidelines on Outsourcing; and
- Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption.

In general, these guidelines provide guidance to FIs on:

- maintaining data, infrastructure and network security;
- sound practices on risk management of outsourcing arrangements; and
- the use of cloud computing platforms.

FIs are encouraged to conduct appropriate due diligence on CSPs and to evaluate the risks before entering into a cloud outsourcing arrangement. The risk assessment should also be performed periodically on existing outsourcing arrangements, as part of the approval, strategic planning, risk management or internal control reviews of the outsourcing arrangements of the FI.

Specific Issues Regarding Personal Data Protection

The transfer limitation obligation under the PDPA requires the contract or BCRs to expressly state the locations to which the personal data may be transferred. However, in the context of a CSP cloud outsourcing arrangement, an organisation may have to agree to a CSP's standard contractual terms, which may include a term that confers discretion onto the CSP as to the exact jurisdictions to which personal data may be transferred.

According to the PDPC's Cloud Services Guidelines, in such a situation, the organisation may be considered to have taken appropriate steps to comply with the transfer limitation obligation if:

- the CSP based in Singapore is certified or accredited as meeting relevant industry standards (such as MTCS Level 3 and ISO 27001); and
- the CSP provides assurances that all the data centres or sub-processors in such overseas locations to which the personal data is transferred comply with these standards.

3. Artificial Intelligence

3.1 Liability, Data Protection, IP and Fundamental Rights

There is currently no specific legislation regulating the use of big data, machine learning and artificial intelligence (AI) technologies in Singapore. However, various government and regulatory agencies have developed non-legally binding frameworks to provide industry guidance on these subjects.

Applicable Frameworks

Examples of these frameworks include:

- the PDPC's Model AI Governance Framework and its companion guide, the Implementation and Self-Assessment Guide for Organisations, which give organisations practical recommendations on implementing ethical principles and adopting responsible AI governance;
- the MAS's Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of AI and Data Analytics in Singapore's Financial Sector, which provide a set of principles for the use of AI in decision making in the provision of financial products and services; and
- the MAS's Veritas Initiative, which assists FIs in evaluating their AI and data analytics solutions against the MAS's FEAT principles.

Notably, the PDPC's Model AI Governance Framework represents the efforts of Singapore's policymakers and regulators to articulate a common approach, and a set of consistent definitions and principles in the governance of AI. Broadly, it sets out principles in four key areas:

- internal governance structures and measures – organisations should ensure that there are clear roles and responsibilities as well as risk management and internal controls in place for the ethical deployment of AI;
- AI decision-making models – organisations should consider the risks of different AI models and determine the appropriate degree of human oversight based on the expected probability and severity of harm;
- operations management – organisations should understand the lineage, provenance and quality of the data used, as well as the transparency of the algorithms chosen; and
- stakeholder interaction and communication – organisations should seek to build trust and maintain open relationships with individuals regarding the use of AI through general disclosure, transparency and policy explanations, and careful design of human-AI interfaces.

On 25 May 2022, the Infocomm Media Development Authority (IMDA) and the PDPC launched AI Verify, which is the world's first AI governance testing framework and toolkit for companies that wish to demonstrate responsible AI in an objective and verifiable manner. Developers and owners can verify the claimed performance of their AI systems against a set of principles through standardised tests. AI Verify packages together a set of open-source testing solutions, including a set of process checks, into a toolkit for convenient self-assessment. The toolkit will generate reports for developers, management and business partners, covering major areas affecting AI performance.

On 7 June 2023, the IMDA set up the AI Verify Foundation (the Foundation) to harness the collective power and contributions of the global open-source community to develop AI Verify. The Foundation seeks to boost AI testing capabilities and assurance to meet the needs of companies and regulators globally. It has more than 60 general members, with seven premier members – Aicadium, Google, IBM, IMDA, Microsoft, Red Hat and Salesforce – that will set strategic directions and a development roadmap for AI Verify.

Singapore's second National AI Strategy (NAIS 2.0) was officially launched on 4 December 2023 and outlines Singapore's vision to be a place where AI serves

as a force for good, where AI is harnessed to uplift Singapore's collective economic and social potential over the next three to five years.

On 1 April 2024, the PDPC published the Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems to provide:

- more clarity for organisations on the use of personal data to train or develop AI to support their efforts to implement AI;
- guidance on information to be provided to consumers when seeking consent;
- guidance to third-party developers of bespoke AI systems who may occupy the role of data intermediaries on their obligations under the PDPA; and
- guidance on best practices to support businesses in their compliance with the PDPA.

Autonomous Vehicles

The Road Traffic (Autonomous Motor Vehicles) Rules 2017 provide that the trial or use of an autonomous motor vehicle on any road is prohibited, unless specific authorisation is obtained. Parties wishing to use such vehicles must submit an application to the Land Transport Authority (LTA), stating matters such as the trial's objectives, the type of autonomous vehicle to be used and its intended purposes. The LTA has the discretion to accept or reject the application and/or impose conditions.

Deepfakes

On 15 October 2024, the Singapore Parliament passed the Elections (Integrity of Online Advertising) (Amendment) Bill, which prohibits the publication of online election advertising containing certain digitally generated or manipulated content about candidates. The Parliamentary Elections Act 1954 and the Presidential Elections Act 1991 will be amended to empower the Returning Officer to issue corrective directions to individuals who publish digitally generated or manipulated online election advertising, to social media services and to internet access service providers to take down offending content or to disable access by Singapore users to such content during election periods.

Fake News

The Protection from Online Falsehoods and Manipulation Act (POFMA) was enacted to prevent the electronic communication in Singapore of false statements of fact, amongst other things. Notably, Section 8 of POFMA prohibits the making or alteration of an automated computer program (ie, an AI "bot") with the intention of using it to communicate or enabling any other person to communicate a false statement of fact in Singapore.

Data Protection

The collection and use of large data sets for big data analytics, machine learning and AI may trigger data protection concerns, especially where such data sets involve personal data (see **2.1 Highly Regulated Industries and Data Protection** for the definition of personal data). Moreover, it is not uncommon for AI systems to utilise data mining solutions to obtain data from third-party sources, in some cases without having obtained consent from the individual affected.

Another significant data protection challenge is the increasing ease with which researchers can re-identify individuals from previously pseudonymised or anonymised data sets by matching them against publicly available information or other data sets.

Intellectual Property

It remains unclear whether and how existing intellectual property frameworks may be applied in protecting AI-generated works. Under Singapore copyright law, the creative elements of a work must be attributable to a natural person in order for copyright protection to vest.

However, AI-related inventions may be patentable. In April 2019, the Intellectual Property Office of Singapore (IPOS) launched an Accelerated Initiative for Artificial Intelligence (AI2) scheme, under which AI-related patent applications may be granted on an accelerated basis if various conditions are satisfied – most notably, the application must be an AI invention. In addition, under the Patents Act 1994, in order for an invention to be patentable, it must be new, involve an inventive step, and be capable of industrial application.

Furthermore, the CA, which came into force on 21 November 2021, includes a new exception to copyright infringement for the purpose of computational data analysis (regardless of whether commercial or non-commercial). This exception allows inventors to use lawfully accessed data in their AI machines for computational data analysis, under certain conditions, without the fear of being liable for copyright infringement.

4. Internet of Things

4.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

Singapore has not enacted any laws that specifically govern the internet of things (IoT), but certain existing laws and regulations may apply to various aspects of IoT projects or applications.

Telecommunications

The IMDA, as established under the Info-communications Media Development Authority Act 2016 (IMDA Act), is responsible for regulating the telecommunications sector in Singapore, amongst others, pursuant to its exclusive privilege under the Telecommunications Act 1999 (TA).

Under the TA, "telecommunications" is defined very broadly as any transmission, emission or reception of signs, signals, writing, images, sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems, whether or not such signs, signals, writing, images, sounds or intelligence have been subjected to rearrangement, computation or other processes by any means in the course of their transmission, emission or reception.

As the primary legislation governing the telecommunications industry in Singapore, the TA sets out the broad licensing and regulatory framework for the telecommunications sector. Unless an exemption applies, the IMDA's jurisdiction may potentially extend to the licensing of IoT projects or applications if such projects or applications may be regarded as involving the operation or provision of telecommunications systems or services under the TA. Where applicable, such persons would therefore need to comply with the general obligations and any specific conditions of approval under their respective licences that have been granted by the IMDA (see **6.1 Scope of Regulation and Pre-Marketing Requirements** for more details on the licensing of telecommunication systems and services).

Data Protection

The applicability of the PDPA may be triggered if the IoT device in question can be used to collect personal data in Singapore and transfer it wirelessly through the network. In such a case, the organisation that collects or transfers the personal data (which may be an IoT service provider) will need to comply with the data protection obligations in respect of such data, unless an exception applies.

Cybersecurity

The Cybersecurity Act 2018 sets out a framework for the designation and monitoring of critical information infrastructure (CII) in essential sectors, such as energy, info-communications, media, water, healthcare, banking and finance, security and emergency services, aviation, land transport, maritime, and services relating to the functioning of the government.

Under the Cybersecurity Act, a computer or computer system may be designated by the Commissioner of Cybersecurity as CII if:

- it is necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore; and
- the computer or computer system is located wholly or partly in Singapore.

Owners of CII are subject to various obligations under the Cybersecurity Act, including reporting cybersecurity incidents, conducting regular cybersecurity audits and risk assessments, and furnishing relevant information.

On 11 April 2022, the licensing framework for cybersecurity service providers came into effect, along with the Cybersecurity (Cybersecurity Service Providers) Regulations 2022. The licensing framework covers

cybersecurity service providers providing penetration testing services and managed security operations centre monitoring services, and aims to improve the standard of cybersecurity service providers and address the information asymmetry between consumers and service providers.

To keep up with the evolving cybersecurity threats and nature of businesses, the Cybersecurity (Amendment) Bill was passed in Singapore Parliament on 7 May 2024 to expand the Cybersecurity Agency of Singapore's oversight beyond owners of CII to:

- essential service providers that use CII owned by a third party;
- major foundational digital infrastructure service providers;
- entities of special cybersecurity interest; and
- owners of systems of temporary cybersecurity concern.

As of 1 January 2025, the amendments have yet to come into force.

With the increasing adoption of IoT solutions amongst various stakeholder groups, including consumers, enterprises and governments, organisations that deploy IoT projects or solutions in the essential sectors discussed above may wish to pay particular attention to the possibility of their systems being designated as CII and subjected to the obligations under the Cybersecurity Act.

4.2 Compliance and Governance

Organisations intending to implement IoT solutions can refer to the following standards published by the IMDA:

- IoT Cyber Security Guide, which provides baseline recommendations, foundational concepts and checklists relating to the security aspects of IoT systems;
- Singapore Standard 695:2023, which identifies common requirements for the interoperability of IoT systems to support a variety of use cases and their integration; and
- Technical Reference 64:2018, which introduces the foundational security concepts and terminology for IoT systems and demonstrates their applications (please note that this Guideline is currently under revision).

While compliance with these standards is not mandatory for organisations implementing IoT solutions, the IMDA encourages organisations to comply with these standards in order to enable an ecosystem of interoperable sensor network devices and systems, reduce deployment costs, and support Singapore's enterprises.

4.3 Data Sharing

Key Legal Requirements

There are no data sharing requirements specifically targeted at organisations implementing IoT solutions. However, where personal data is collected by the IoT devices before being transferred wirelessly through the network, organisations that employ IoT solutions will have to comply with the following obligations under the PDPA (among others).

- Consent Obligation: Section 13 of the PDPA prohibits the collection, use or disclosure of personal data unless the individual gives or is deemed to have given his or her consent, or unless the collection, use or disclosure without the individual's consent is required or authorised under the PDPA or any other written law. In the second instance, the PDPA sets out the circumstances or purposes (in its First and Second Schedules) where the consent of an individual is not required for the processing of his or her personal data.
- Protection Obligation: Section 24 of the PDPA requires organisations to make reasonable security arrangements to protect personal data in their possession or under their control in order to prevent:
  (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and
  (b) the loss of any storage medium or device on which personal data is stored.

Specific Categories of Personal Data

While the PDPA does not define "sensitive" personal data nor prescribe different legal bases for its collection, the PDPC has taken the position that certain types of personal data (eg, personal data of a financial

nature such as bank account details, personal data of minors and health and medical information) should be safeguarded by a higher level of protection so as to constitute "reasonable security measures" under the PDPA (Re Aviva Ltd [2017] SGPDPC 14).

5. Audiovisual Media Services

5.1 Requirements and Authorisation Procedures

Regulation of the Media Sector

Similar to telecommunications, the IMDA is also responsible for the regulation of the media sector (including broadcasting and film). "Media" is defined in the IMDA Act as:

- a film, as defined in the Films Act 1981 (FA);
- a newspaper, as defined in the Newspaper and Printing Presses Act 1974;
- a broadcasting service, as defined in the Broadcasting Act 1984 (BA);
- a publication, as defined in the Undesirable Publications Act 1967; or
- such other medium of communication of information, entertainment or other matter to the public (or a section of the public) as the Minister may specify by order in the Gazette.

Generally, the provision of audiovisual services in or from Singapore (eg, TV or radio) would be regulated under the BA, and the IMDA may grant a broadcasting licence for the provision of:

- free-to-air nationwide, localised and international television services;
- subscription nationwide, localised and international television services;
- special interest television services;
- free-to-air nationwide, localised and international radio services;
- subscription nationwide, localised and international radio services;
- special interest radio services;
- audiotext, videotext and teletext services;
- video-on-demand services;
- broadcast data services; and
- computer online services.

In addition, the BA provides for a class licensing regime, under the Broadcasting (Class Licence) Notification and Broadcasting (Class Licence – Broadcasting to Digital Display Panels) Notification 2020, for:

- virtual area network computer online services;
- computer online services that are provided by internet content providers and internet service providers (ISPs); and
- distribution network digital display panels services.

In particular, it should be noted that "internet content providers" is broadly defined under the Broadcasting (Class Licence) Notification to include any individual in Singapore who provides any programme, for business, political or religious purposes, on the World Wide Web through the internet, as well as any corporation or group of individuals (whether registrable or incorporated under Singapore law or not) that provides any programme on the World Wide Web through the internet.

In such cases, it is possible that companies operating video-sharing platform services on YouTube, for example, may be automatically deemed to be class-licensed, and must comply with the conditions of the class licence and the Internet Code of Practice. Amongst other requirements, broadcasting class licensees may be asked by the IMDA to remove or prohibit the broadcast of certain programmes the IMDA has deemed to be against the public interest, public order or national harmony or to offend against good taste or decency.

Furthermore, as of 1 February 2023, the amended BA contains measures to regulate providers of online communication services (OCS). The IMDA will also be empowered to issue directions to deal with egregious content that can be accessed by Singapore users on an OCS (see **10.1 Laws and Regulations for Social Media** for more details on the Online Safety Act).

Eligibility, Fees and Charges

In general, broadcasting companies are required to be Singapore-incorporated companies or the registered local branches of a foreign company in order to hold a "relevant licence" (unless exempted by the Minister for Communications and Information). A "rel-

evant licence" (which excludes class licences) refers to any free-to air licence or any broadcasting licence under which a subscription broadcasting service may be provided, and which permits broadcasts that are capable of being received in 50,000 dwelling houses or more.

Different types of broadcasting licences may come with different licence fees, as follows:

- for free-to-air nationwide television service licences, licensees must pay 2.5% of their total revenue or SGD250,000 per annum, whichever is higher, and provide a performance bond of SGD200,000;
- for free-to-air nationwide radio service licences, licensees must pay 2.5% of their total revenue per annum and provide a performance bond of SGD200,000 in the form of a banker's guarantee;
- for subscription international television service licences (for satellite television service broadcasters), licensees must pay SGD5,000 per annum and provide a performance bond of SGD50,000 in the form of a banker's guarantee if they are not based or registered in Singapore;
- for nationwide subscription television service licences, licensees must pay 2.5% of their total revenue or SGD50,000 per annum, whichever is higher, and provide a performance bond of SGD200,000; and
- for niche television service licences (which applies to providers of television services targeting niche market segments and over-the-top television services delivered through the internet), no licence fee is required.

For completeness, yearly fees are payable for certain types of services under the Broadcasting (Class Licence) Notification, as follows:

- teletext services – SGD2,000;
- computer online services by internet access service providers – SGD1,000;
- computer online services by non-localised internet service resellers – SGD100 (if fewer than 500 user accounts) or SGD1,000 (for 500 accounts or more); and
- computer online services by localised internet service resellers – SGD100 for each premises at which the computer online services are provided.

6. Telecommunications

6.1 Scope of Regulation and Pre-Marketing Requirements

As noted in the definition of "telecommunications" (see **4.1 Machine-to Machine Communications, Communications Secrecy and Data Protection**), the licensing and regulatory framework for telecommunication systems and services under the TA is sufficiently broad to cover almost every technological application, even if there are no specific references to individual applications such as RFID tags, Voice over Internet Protocol (VoIP) or instant messaging. That said, service-specific issues may be covered in various regulations, codes of practice, standards of performance, directions, advisory guidelines and licences issued by the IMDA pursuant to its powers under the TA.

For instance, issues pertaining to the licensing and use of the radio frequency (RF) spectrum and the operation of radio stations and networks are regulated under the Telecommunications (Radio-communication) Regulations, while the Telecommunications (Dealers) Regulations set out the framework in relation to the manufacturing, importation and sale (amongst other things) of telecommunication equipment.

The IMDA was formally established on 1 October 2016 as a converged regulator for both the info-communications and media sectors but, in general, the telecommunications and media sectors continue to be governed by separate regulatory frameworks. For instance, the TA does not currently apply to the licensing of broadcasting services or any broadcasting apparatus, which instead falls under the BA.

On 2 May 2022, the Code of Practice for Competition in the Provision of Telecommunication and Media Services 2022 came into operation. It was issued by the IMDA to promote the efficiency and competitiveness of the media and telecommunications industry.

Licensing for the Operation and Provision of Telecommunication Systems and Services

Generally, licences for the operation and provision of telecommunication systems and services in Singapore would fall into one of two categories: facilities-based operations (FBOs) or services-based operations (SBOs). Where RF spectrum is required for the provision of wireless services, additional licensing is required under the Telecommunications (Radio-communication) Regulations.

Taking the provision of VoIP services as an example, it is noted in the IMDA's Guidelines on Licensing and Regulatory Framework for IP Telephony Services in Singapore that applicants need to first obtain either an FBO or SBO licence from the IMDA in order to provide IP telephony services. IP telephony services are defined as any VoIP services offered using an E.164 telephone number allocated to customers in Singapore, which allow customers to make and receive voice, data and/or video calls using the same IP telephone number from any domestic or overseas location where broadband internet access is available.

An FBO licence is required if applicants intend to deploy and/or operate any form of telecommunication networks, systems and/or facilities for the purpose of providing telecommunication (eg, IP telephony services) and/or broadcasting services outside of their own property boundaries to third parties (which may include other licensed telecommunication operators, business customers or the general public).

In contrast, only an SBO licence is required if applicants intend to lease telecommunication network elements from any FBO licensee to provide telecommunication services (eg, IP telephony services), or to resell the telecommunication services of such FBO licensees to third parties.

While there are two licensing schemes under the SBO framework (ie, class licensing and individual licensing), operators that lease international transmission capacity for the provision of their services are usually required to obtain an SBO (Individual) Licence. The SBO (Class) Licence is a licensing scheme where the terms and conditions are gazetted in the Telecommunications (Class Licences) Regulations.

Anyone who provides services within the scope of the SBO (Class) Licence will be deemed to have read and agreed to the terms and conditions of the class licence.

The IMDA's licensing framework is formulated on a hierarchical basis, with FBO licences placed on a higher level than SBO licences. This means that FBO licensees are able to offer telecommunication services that would ordinarily require an SBO licence without having to obtain a separate SBO licence, but not vice versa. If an SBO licensee subsequently wishes to undertake FBO-related activities (such as deploying or operating any telecommunication network, systems or facilities), it will need to apply for a new FBO licence to replace its existing SBO licence.

Eligibility, Fees and Charges

In terms of eligibility, the IMDA's current practice is to issue FBO licences only to Singapore-incorporated companies, although such companies can be wholly owned by a foreign entity. In the case of SBO (Individual) licences, local registered branches of foreign companies are eligible to apply, while SBO (Class) licences may also be held by limited liability partnerships or limited partnerships. Further details regarding the application process for an FBO or SBO licence and the information required can be found in the respective application guidelines issued by the IMDA on its website.

In terms of applicable fees and charges, FBO licensees are subject to a minimum annual recurrent licence fee of SGD80,000 or SGD200,000 (depending on whether the licensee is an FBO or a designated public telecommunication licensee), with further fees chargeable as a percentage of their incremental annual gross turnover (AGTO) exceeding SGD50 million as follows:

- 0.8% of the incremental AGTO between SGD50 million and SGD100 million; and
- 1% of the incremental AGTO above SGD100 million.

SBO (Individual) licensees are subject to a minimum annual recurrent licence fee of SGD4,000, with further fees chargeable as a percentage of their incremental AGTO exceeding SGD50 million as follows:

- 0.5% of the incremental AGTO between SGD50 million and SGD100 million; and
- 0.8% of the incremental AGTO above SGD100 million.

At the time of writing, there are no annual recurrent licence fees for SBO (Class) licensees. Depending on the type of services provided, SBO (Class) licensees may need to make a one-time payment of SGD200 upon registration with the IMDA.

6.2 Net Neutrality Regulations

The IMDA adopts a three-pronged approach to net neutrality in Singapore, which aims to:

- facilitate a competitive internet access market;
- improve information transparency so that consumers can better understand the various internet broadband service choices when selecting an internet broadband package; and
- protect consumer interests and ensure that consumers enjoy a reasonable quality of internet access.

The IMDA's policy framework on net neutrality sets out five main requirements:

- ISPs and telecom network operators are prohibited from blocking legitimate internet content or imposing discriminatory practices, restrictions, charges or other measures that will render any legitimate internet content effectively inaccessible or unusable;
- ISPs and telecom network operators must comply with the IMDA's competition and interconnection rules in the Converged Code of Practice for Competition in the Provision of Telecommunication and Media Services (TMCC);
- ISPs and telecom network operators must comply with the IMDA's requirements as to information transparency and disclosure to end users of network management practices and typical internet broadband download speeds;
- ISPs must meet the minimum broadband quality of service standards prescribed by the IMDA – reasonable network management practices are permitted, provided that the minimum broadband quality of service requirements are adhered to, and that such practices will not render legitimate internet content unusable; and
- ISPs and telecom network operators are allowed to offer niche or differentiated services that meet the IMDA's information transparency, minimum quality of service and fair competition requirements.

6.3 Emerging Technologies

Please see **4.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection**.

7. Challenges With Technology Agreements

7.1 Legal Framework Challenges

Data Security

One challenge that some organisations may face when entering into IT service agreements relates to obligations surrounding data security, particularly where personal data is involved. It is common for organisations seeking to engage third-party IT service providers to enter into a written data processing agreement that sets out each party's roles and responsibilities in relation to the personal data in question, as well as the specific security measures that would be put in place.

In addition, the PDPC requires organisations to design and organise their security arrangements to fit the nature of the personal data held by the organisation and the possible harm that might result from a security breach, and to identify reliable and well-trained personnel responsible for ensuring information security.

In cases where the contract for IT services is with an FI, for instance, the organisation should be aware that FIs in Singapore are also subject to the regulations and guidelines promulgated by the MAS. These regulations and guidelines include but are not limited to the MAS's Guidelines on Outsourcing, Notice on Technology Risk Management, Notice on Cyber Hygiene, and Technology Risk Management Guidelines, which, amongst other things, may require FIs to exercise strong oversight of arrangements with third-party service providers to ensure system resilience and maintain data confidentiality and integrity. As a result, organisations entering into IT service agree-

ments with FIs may need to include applicable provisions in relation to the conduct of security audits and reporting with regard to breaches or cyber-attacks.

Data Localisation

In Singapore, there are no express laws in relation to data localisation or data residency. The PDPC has notably taken a stance against data localisation and emphasised the importance of the free flow of data through coherent and efficient cross-border data transfer mechanisms.

Where the IT service agreement involves a cross-border transfer of personal data (eg, the storage of data in the cloud or in a data centre located outside of Singapore, or if the solution involves cloud computing), the organisation should also consider compliance with cross-border data transfer requirements under the PDPA and PDPR; see **2.1 Highly Regulated Industries and Data Protection** (Specific Issues Regarding Personal Data Protection) for more details on the transfer limitation obligation and specific issues for CSPs.

7.2 Service Agreements and Interconnection Agreements

While telecommunications licensees are free to negotiate favourable terms in interconnection and access agreements, the IMDA regulates interconnection and access issues pursuant to the TMCC. The TMCC provides that FBO licensees and SBO licensees using switching or routing equipment to provide services to the public are under a general duty to interconnect with one another. Interconnection agreements must be submitted to the IMDA. While the IMDA generally does not involve itself in interconnection negotiations between non-dominant licensees, an interconnection agreement between non-dominant licensees must nevertheless fulfil certain minimum interconnection duties as specified in the TMCC, and the IMDA reserves the right to reject an interconnection agreement between non-dominant licensees that does not fulfil the requirements.

Licensees have a duty to co-operate in good faith and in a commercially reasonable manner in implementing the terms of their interconnection agreements, avoiding unnecessary disputes and resolving any disputes promptly and fairly. The IMDA generally recognises that interconnection agreements are private contracts between licensees, and will not involve itself in disputes arising from interconnection agreements where both parties are non-dominant licensees.

Licensees who wish to interconnect with dominant licensees may generally do so under one of three options:

- pursuant to a reference interconnection offer (RIO) approved by the IMDA;
- on the same prices, terms and conditions that a dominant licensee has agreed to with another similarly situated licensee; or
- pursuant to the prices, terms and conditions of an individualised interconnection agreement between the two parties.

The IMDA has published the above agreements between dominant licensees and companies on its website, as well as model agreements. Companies are encouraged to refer to the terms in the published agreements during their negotiations with dominant licensees.

Licensees classified by the IMDA as dominant licensees are required to publish RIOs, under which they offer interconnection-related services and mandated wholesale services on prices, terms and conditions that are pre-approved by the IMDA, unless specifically exempted by the IMDA. A telecommunication licensee will be classified by the IMDA as dominant if:

- it is licensed to operate facilities used for the provision of telecommunication services that are sufficiently costly or difficult to replicate, such that requiring new entrants to do so would create a significant barrier to rapid and successful entry into the telecommunication market in Singapore by an efficient competitor; or
- it has the ability to exercise significant market power in any market in Singapore in which it provides telecommunication services.

Licensees currently classified as dominant licensees include:

- Singtel;

- StarHub Cable Vision;
- NetLink NBN Management Pte Ltd (as trustee-manager of NetLink NBN Trust); and
- NetLink Management Pte Ltd (as trustee of NetLink Trust).

8. Trust Services and Digital Entities

8.1 Trust Services and Electronic Signatures/ Digital Identity Schemes

Digital Identity

Launched in 2003, SingPass is a secure personal authentication system that allows users to access various government services online. Under the National Digital Identity initiative, SingPass, MyInfo (a service that automatically fills out selected personal details for online forms) and MyInfo Business (a service that enables a business to manage the use of its corporate and applicant's personal data for simpler online transactions) were brought together to provide greater transactional security and ease of use. All SingPass users are automatically provided with a MyInfo profile, which allows them to provide personal data once to digital services and then consent to have their personal data retrieved from government sources to pre-fill forms for digital transactions.

As SingPass and MyInfo are managed by the Government Technology Agency ("GovTech"), the data protection provisions in the PDPA do not apply to them and other public agencies. Instead, data management by public agencies is governed by the Public Sector (Governance) Act 2018 and guided by the Government Instruction Manual on Infocomm Technology & Smart Systems Management (previously known as IM8).

However, private organisations utilising SingPass and MyInfo to facilitate their transactions are subject to the obligations under the PDPA. As personal data on these platforms is often sensitive data, organisations should take the sensitivity of the personal data into account and implement robust policies and procedures to ensure appropriate levels of protection and security.

Electronic Signatures

The ETA makes a distinction between electronic signatures, secure electronic signatures and digital signatures.

An electronic signature could conceivably take various forms, such as a scanned physical signature or typing one's name where a signature is required.

According to Section 18 of the ETA, an electronic signature will be recognised as a "secure electronic signature" if, through the application of a specified security procedure or a commercially reasonable security procedure agreed to by the parties, it can be verified that, at the time the signature was made, it was:

- unique to the person using it;
- capable of identifying such person;
- created in a manner or using a means under the sole control of the person using it; and
- linked to the electronic record to which it relates in a manner such that if the record were changed the electronic signature would be invalidated.

The key difference between a secure electronic signature and an electronic signature is that the former raises the following statutory presumptions pursuant to Section 19 of the ETA:

- in any proceedings involving a secure electronic record, it is presumed – unless evidence to the contrary is adduced – that the secure electronic record has not been altered since the specific point in time to which the secure status relates; and
- in any proceedings involving a secure electronic signature, it is presumed – unless evidence to the contrary is adduced – that the secure electronic signature is the signature of the person to whom it relates, and that the secure electronic signature was affixed by that person with the intention of signing or approving the electronic record.

Furthermore, the ETA defines a digital signature as an electronic signature consisting of a transformation of an electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can accurately determine whether:

- the transformation was created using the private key that corresponds to the signer's public key; and
- the initial electronic record has been altered since the transformation was made.

A digital signature can be treated as a secure electronic signature if it was created during the operational period of a valid certificate and is verified by reference to the public key listed in such certificate. The certificate must also meet the prescribed requirements under the ETA and be considered trustworthy.

On 5 November 2020, GovTech launched the "Sign with SingPass" service. This was rolled out through GovTech's subsidiary, Assurity Trusted Solutions, which is an accredited Certification Authority under the ETA. The "Sign with SingPass" service allows SingPass users to electronically sign certain documents with some government agencies and private sector businesses. Signatures made using the "Sign with SingPass" service can be regarded as secure electronic signatures under the ETA. However, the use of electronic or digital signatures in the following matters warrants further consideration:

- the creation or execution of a will;
- the creation, performance or enforcement of an indenture, a declaration of trust or a power of attorney, with the exception of implied, constructive and resulting trusts;
- any contract for the sale or other disposition of immovable property or any interest in such property; and
- the conveyance of immovable property or the transfer of any interest in immovable property.

On 2 August 2023, the Oaths, Declarations and Notarisations (Remote Methods) Bill and the Constitution of the Republic of Singapore (Amendment No 2) Bill were passed in Parliament. The Bills seek to introduce the option of making statutory declarations, oaths and affirmations and to notarise documents through remote means, in line with the government's ongoing efforts to facilitate electronic transactions, so as to implement greater convenience and efficiency for individuals and businesses in Singapore.

9. Gaming Industry

9.1 Regulations

In relation to video gaming, the FA will be relevant. Where games include features such as specific in-game purchases, loot boxes and gambling elements, the Gambling Control Act 2022 (GCA) may be relevant.

Films Act 1981

The FA regulates, inter alia, the possession, importation, distribution and exhibition of films in Singapore. Under the FA, "film" is broadly defined to include a video game; accordingly, video games in Singapore may be regulated under the FA and be subject to the IMDA's classification guidelines and regulations.

Under the FA, "video game" expressly excludes a video game made available by means of a computer online service that is a broadcasting service and is played:

- on a mobile device or other device onto which the video game has been installed; or
- while the player is using a broadcasting service that enables end users to access the internet.

Any person who in the course of any business imports, distributes or publicly exhibits films is required to obtain a licence. With certain exceptions, all films and videos distributed and exhibited in Singapore must be submitted to the IMDA for classification and certification.

Distributors of offline single-player video games are automatically class-licensed, and must enforce the relevant age restrictions and adhere to the licence conditions, as well as any additional classification conditions imposed by the IMDA. Video games that contain classifiable elements will be rated Advisory 16 or Mature 18, and will need to be affixed with the corresponding rating labels and consumer advice.

The IMDA's Video Game Classification Guidelines set out the general principles and content concerns that the IMDA considers in its classification process and aims to reflect community standards. In general, the IMDA's classification process is guided by the following principles:

- generally accepted social norms and values;
- the need to protect the young;
- racial/religious harmony;
- public order and national interest;
- the treatment of theme and content; and
- the evaluation of impact.

Gambling, Loot Boxes, In-Game Purchases

Games that feature specific in-game purchases could potentially fall under the scope of the GCA. Under the GCA, "gambling" is defined as the act of betting, playing a game of chance for a prize or playing a gaming machine, and participating in a lottery. In Singapore, only social gambling, gambling with licensed operators and jackpot gambling in private clubs are allowed. Online gambling is currently prohibited in Singapore, unless licensed or exempted.

Persons who offer interactive games of chance that are played for a prize and are conducted in Singapore, or can be accessed by or delivered to players physically in Singapore, may fall under Type 1 or 2 Class Licences under the Under the Gambling Control (Remote Games of Chance – Class Licence) Order 2022 (GCO) and be subject to conditions subsequent of the class licences. Class licensees who contravene any of the conditions subsequent may be liable for regulatory sanctions by the Gambling Regulatory Authority (GRA).

Games that fall under the Type 1 Class Licence are free of charge and must not involve the use, design elements or mechanics of prohibited games specified in the First Schedule of the GCO, nor the image of gambling articles specified in the Second Schedule of the GCO.

Conditions subsequent of the Type 1 Class Licence include ensuring that promotional materials are free of specified gambling articles, and that complimentary tokens given to players to play the game are consumable and restricted to unique use by each individual player and cannot be transferred to any other person.

Games that fall under the Type 2 Class Licence provide prizes that are not money, may be won or acquired from in-game microtransactions or by playing the game, and are designed primarily for use in the same or related interactive games.

Conditions subsequent of the Type 2 Class Licence include taking all reasonably practicable steps to not provide any service making any prize, feature or complimentary token given by the licensee readily convertible into money or money equivalent, or anything else of value, except for use in in-game microtransactions in the same or related interactive games.

Chance-based loot boxes (as long as there are no in-game monetisation facilities) are not currently regulated under the GCA as a form of gambling, as long as there are no in-game monetisation features.

9.2 Regulatory Bodies

The regulatory body overseeing the classification, import, distribution and public exhibition of video games in Singapore is the IMDA. Insofar as the games feature content that involves regulated subject matter under the GCA, the GRA will be the regulatory body.

On a non-exhaustive basis, the enforcement powers of the relevant regulatory bodies include the following.

- Under Section 11 (1) of the FA, the IMDA is empowered to take regulatory action against licensees for contravention of a condition of their licence or an offence under the FA (such as importing, distributing or publicly exhibiting video games in Singapore in the course of any business without a licence), among others. At the time of writing, details of enforcement action in this front are not published on the IMDA website.
- Under Section 88 (1) of the GCA, the GRA is empowered to revoke or disapply licences granted under the GCA if the licensee has contravened or failed to comply with its licence conditions, the provision of a standard applicable to the licensee, or any direction given to the licensee in lieu of a licence revocation, among other measures. At the time of writing, details of enforcement action on this front are not published on the GRA website.

9.3 Intellectual Property

IP challenges faced by game developers in Singapore include video game cloning and game content rights.

Copyright Protection and Infringement

Video games typically comprise multiple IP protectible components, such as music, art, plot and source code. Examples of works protected by the CA include:

- an authorial work – ie, a literary, dramatic, musical or artistic work (Section 9 of the CA);
- a published edition of an authorial work;
- a sound recording;
- a film;
- a broadcast; or
- a cable programme.

To protect their IP in a virtual environment, game developers will first need to establish authorship and ownership of copyright in the work in question.

For there to be copyright infringement, a qualitatively substantial amount of the original work must have been copied. For example, in the context of video game cloning, this can stray into copyright infringement territory if the creative aspects of the game are copied.

Under the CA, a compilation of data may be protected as a literary work if it constitutes an intellectual creation by reason of the selection or arrangement of its contents. In the context of compilations, the compiler must have exercised sufficient creativity in selecting or arranging the material within the compilation to cloak the original expression with copyright. Thus, it has been held by the Singapore courts in a case involving two publishers of phone directories that such data is not protected by copyright law (see Global Yellow Pages Ltd v Promedia Directories Pte Ltd [2017] 2 SLR 185).

That said, in Singapore, the extent of copyright protection over modern-day video games has yet to be conclusively determined. It remains to be seen, in the context of video games, what level of creativity is necessary for a selection or arrangement of facts or data to receive copyright protection.

Trade Mark Issues

Apart from copyright issues, identifying signs or indicia such as video game titles, logos and gamer tags may also be protected under Singapore trade mark law. The key question to consider is whether the game developer owns registered trade marks that cover the video games or similar goods/services.

If any signs have been created through the development of the video game, the video game developer may wish to register such trade marks under the Singapore Trade Marks Act 1998, as the registration of a trade mark over these signs would confer on the game developer exclusive rights to use and authorise others to use the trade mark in relation to the video game (Section 26 of the TMA). In 2023, IPOS published a Circular clarifying its practice on the classification of NFTs and metaverse-related goods and services in an application for registration of a trade mark.

10. Social Media

10.1 Laws and Regulations for Social Media

Online Safety Act

The Online Safety Act introduced new provisions to the BA to regulate OCS accessible by Singapore end users. Currently, social media services are the only regulated OCS. OCS are an electronic services (or parts of an electronic service) that have the characteristics of a social media service, which may be provided in or from Singapore, or from outside Singapore. OCS enable end users to access or communicate content on the internet, or to deliver content to end users.

Under the amended BA, OCS with significant reach and impact in Singapore may be designated as Regulated Online Communication Services. The providers of such Regulated Online Communication Services have the duty to take all reasonably practicable steps to comply with the applicable Codes of Practice, to implement measures to mitigate the risks of danger to Singapore users from exposure to harmful content and to provide accountability to their users on such measures.

On 18 July 2023, the Code of Practice for Online Safety (Online Safety Code) took effect. It seeks to minimise Singapore users' exposure to harmful content, with additional protection for children, by requiring designated social media services to put systems and processes in place to curb the spread of harmful

content on their services, among other measures. The categories of harmful content covered by the Online Safety Code are:

- sexual content;
- violent content;
- suicide and self-harm content;
- cyberbullying content;
- content endangering public health; and
- content facilitating vice and organised crime.

Online Criminal Harms Act

In light of the proliferation of scams and malicious cyber-activities, the Online Criminal Harms Act 2023 (OCHA) was passed in Parliament on 5 July 2023 to counter online criminal activity and protect against online harms. In particular, the OCHA allows directions to be issued to online service providers, other entities or individuals, when there is reasonable suspicion that an online activity is in furtherance of the commission of specified criminal offences.

Designated OCS providers will have to comply with the requirements under the Code of Practice for Online Communication Services (Online Communication Code), which defines "online communication service" as any online service that enables users to access or communicate information with other users by means of the internet.

Under the Online Communication Code, designated providers of OCS must implement appropriate systems, processes or measures to achieve the following objectives:

- quick disruption of malicious accounts and activities;
- deployment of safeguards to prevent propagation of malicious activities; and
- accountability.

In brief, such providers are required to implement reasonable verification measures to prevent the creation and usage of inauthentic accounts or bots for scams and malicious cyber activities. Furthermore, such providers are to proactively detect and take necessary action(s) against suspected scams and malicious cyber activities. They must also submit an annual report on the implementation of the measures and efforts to meet the objectives.

Currently, designated online services include social media services such as Facebook and Instagram, alongside online messaging applications such as Telegram, WeChat and WhatsApp.

10.2 Regulatory and Compliance Issues

Under the new Part 10A of the BA, the IMDA is empowered to issue directions to deal with egregious content that can be accessed by Singapore users on OCS. For instance, the IMDA may issue directions to an OCS provider to disable access by Singapore users to the egregious content on the service or to ensure that a specified account cannot continue to communicate to Singapore users. Moreover, the amended BA empowers the IMDA to issue directions to internet access service providers to block access by Singapore users to the non-compliant OCS if an OCS provider fails to comply with the IMDA's direction.

Online Criminal Harms Act

Under Part 2 of the OCHA, providers of an online service can be subject to a disabling direction or account restriction direction if users misuse or share illegal content on the online service.

A disabling direction or account restriction direction in respect of online activity may be issued if it is:

- reasonably suspected that a specified offence has been committed and that any online activity is in furtherance of the commission of the offence; or
- suspected or there is reason to believe that any online activity is preparatory to, or in furtherance of, the commission of a scam or malicious cyber activity offence.

A disabling direction under Section 9 of the OCHA will require the online service provider to take all reasonable steps to disable access by Singapore persons to:

- any relevant material stored, posted, provided or transmitted on or through the online service;
- any identical copies of the relevant material stored, posted, provided or transmitted on or through the online service; and

• any relevant location on the online service.

Meanwhile, an account restriction direction under Section 11 of the OCHA will require the online service provider to take all reasonable steps to disallow or restrict interaction between any relevant account on the online service and Singapore persons, by the time specified in the direction. Reasonable steps may include the termination, suspension or restriction of one or more functionalities of the online service in relation to the relevant account.

Given that the regulations in relation to social media services are relatively nascent, there have not been any published enforcement decisions with respect to social media as of 1 January 2025.

11. Data Privacy and Cybersecurity

11.1 Data Privacy in Telecommunications

No content provided in this jurisdiction.

11.2 Cybersecurity in Digital Media and Streaming Services

No content provided in this jurisdiction.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com