Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Artificial Intelligence 2024

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

Singapore: Law and Practice & Trends and Developments

Lim Chong Kin and Cheryl Seah
Drew & Napier LLC

SINGAPORE

Law and Practice

Contributed by:
Lim Chong Kin and Cheryl Seah
Drew & Napier LLC

Contents

Drew & Napier LLC is a full-service Singapore law firm, which was founded in 1889 and remains one of the largest law firms in the country. Drew & Napier has a highly regarded TMT practice group, which consistently ranks as the leading TMT practice in Singapore. The firm possesses unparalleled transactional, licensing and regulatory experience in the areas of telecommunications, technology, media, data protection and cybersecurity. The TMT practice is supported by more than ten lawyers and paralegals with extensive experience in info-communications, data protection, technology, and sector-specific and general competition law. The TMT practice acts for a broad range of clients, spanning multinational corporations and local companies across industries. These clients include global and regional telecommunications service providers, sectoral regulators (both local and foreign), consultants, software houses, hardware manufacturers, and international law firms.

Authors

Lim Chong Kin is the managing director of Drew & Napier's corporate and finance department, head of the firm's TMT practice, and co-head of both its data protection, privacy and cybersecurity practice and its competition law and regulatory practice. With a strong background in competition, data protection and technology laws, he is often depended upon by clients to deliver commercially savvy advice, especially in the cutting-edge fintech and AI industries. Chong Kin has in-depth expertise and experience in competition law matters, in particular. Since 1999, he has advised the sectoral competition regulators on liberalisation matters, including drafting, implementing and enforcing the competition law framework for the telecommunications, media and postal sectors.

Cheryl Seah is a director of the corporate and finance department at Drew & Napier. Cheryl advises companies ranging from Fortune 500 multinational corporations to local and foreign start-ups on legal and governance issues at all stages of the AI life cycle – from procuring the computing resources, to the data used in model training, to the IP and liability issues arising from the output. She publishes frequently with the Law Society of Singapore on legal issues arising from the use of AI and has conducted talks on AI for external organisations (including a university) and regulators in South-East Asia. In her previous role in the Attorney-General's Chambers (Singapore's central law drafting office), she has drafted legislation across a wide variety of subjects, focusing on transport (including autonomous vehicles), infrastructure, technology and civil procedure.

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. General Legal Framework

1.1 General Legal Background

Singapore unveiled its first National AI strategy in 2019, with the aim of becoming a leader in developing and deploying scalable, impactful AI solutions in key sectors of high value and relevance to citizens and businesses by 2030. With AI going "mainstream" with the release of ChatGPT by OpenAI in November 2022, Singapore's National AI Strategy was updated in December 2023 (the "NAIS 2.0"), with AI now positioned as a necessity that people "must know", rather than just "good to have". Singapore will also take a global approach to AI, in terms of co-operating both to innovate and also to overcome the challenges brought about by AI (eg, energy, data and ethics).

Singapore has not enacted any laws concerning the use of AI in general. However, the following laws address specific applications of AI, which are detailed further in **3.2 Jurisdictional Law**.

- Singapore's Road Traffic Act 1961 was amended in 2017 in order to provide a regulatory sandbox for the trial and use of autonomous motor vehicles, which was previously done by way of exemptions.
- The Health Products Act 2007 (HPA) requires medical devices incorporating AI technology (AI-MD) to be registered before they are used (see **14.3 Healthcare** for further details).

Organisations must comply with relevant laws when deploying AI technology – for example, laws relating to safety, personal data protection and fair competition. Where the use of AI results in harm, existing legal principles (such as tort liability and contractual liability) will still apply.

Singapore also has a set of voluntary guidelines in place for both traditional/predictive AI (which makes predictions based on historical data instead of creating new content) and generative AI, as follows.

For traditional/predictive AI:

- the Model Artificial Intelligence Governance Framework (Second Edition) (the "Model Framework") issued by the Infocomm Media Development Authority (IMDA) and the Personal Data Protection Commission (PDPC) in 2020, which states that the use of AI should be fair, explainable, transparent and human-centric;
- the Implementation and Self-Assessment Guide for Organisations (ISAGO) – a compan-

ion to the Model Framework issued in 2020 – which sets out questions and examples for organisations to rely on when self-assessing how their AI governance practices align with the Model Framework; and
- "AI Verify" (an AI governance testing framework and toolkit rolled out in May 2022, comprising both technical tests and process checks for organisations to assess their AI systems against 11 internationally-accepted AI ethics principles), which has since been mapped to the US National Institute of Standards and Technology's AI Risk Management Framework in October 2023 – both the Singapore and US frameworks are aligned (ie, interoperable), thereby reducing compliance costs for organisations to meet the requirements within both frameworks.

For generative AI:

- the IMDA first issued a paper – "Generative AI: Implications for Trust and Governance" – in June 2023, outlining six key risks brought about by generative AI and measures to address them;
- the IMDA then issued (in October 2023) a paper on baseline standards for evaluating large language models (LLMs), titled "Cataloguing LLM Evaluations"; and
- the Model AI Governance Framework for Generative AI (the "Model Gen-AI Framework") – setting out nine dimensions to build trustworthy generative AI, as well as the actions the industry and policymakers must take to achieve it – was released on 16 January 2024 for public consultation up to 15 March 2024 and was finalised on 20 May 2024.

Regulators also issue guidance notes to organisations, such as the following – of which, the first three are for general application, and the final two apply to specific industries.

- The PDPC released the Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems in March 2024 (the "PDPC AI Advisory Guidelines"), following its public consultation in July 2023.
- The Intellectual Property Office of Singapore (IPOS) issued the IP and Artificial Intelligence Information Note to provide an overview of how AI inventions can receive IP protection.
- The Cybersecurity Agency of Singapore has collaborated with international partners in producing guidance to organisations on how to use AI systems securely – eg, the "Engaging with Artificial Intelligence" publication led by the Australian Signals Directorate, as well as the "Guidelines for secure AI system development" led by the UK National Cyber Security Centre.
- The Monetary Authority of Singapore (MAS) released the Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector for voluntary adoption by firms providing financial products and services.
- The Ministry of Health (MOH), the Health Sciences Authority (HSA) and the Integrated Health Information Systems co-developed the Artificial Intelligence in Healthcare Guidelines in order to set out good practices for AI developers and complement the HSA's regulation of medical devices incorporating AI technology (AI-MDs).

2. Commercial Use of AI and Machine Learning

2.1 Industry Use

AI is deployed widely across industries in Singapore, from finance to healthcare to food service in restaurants. The revised NAIS 2.0 encourages AI innovation and adoption across all sectors, with a focus on manufacturing, financial services, transport and logistics, and biomedical sciences.

The IMDA/PDPC have also published a Compendium of AI Use Cases (in two volumes) to demonstrate how the Model Framework's AI governance principles have been applied by organisations.

2.2 Involvement of Governments in AI Innovation

Singapore's government announced during the Budget speech in February 2024 that it will be investing more than SGD1 billion during the next five years to boost its AI computing resources, talent pool and industry development. Some initiatives include investing up to SGD500 million to secure the high-performance compute resources required for running AI systems, as well as more than SGD20 million in the next three years to fund additional SG Digital Scholarships for Singaporeans to pursue AI-related courses in universities and overseas internships.

The government is also helping businesses to adopt AI technology. The IMDA and Enterprise Singapore have launched a sandbox in February 2024 for SMEs to trial generative AI solutions for their businesses (eg, in marketing and sales or customer engagement) over a three-month period, with government funding.

3. AI-Specific Legislation and Directives

3.1 General Approach to AI-Specific Legislation

Singapore's approach to regulating AI is that of "agility", as set out in its NAIS 2.0. Singapore's priority is to deepen our understanding of AI and discover and address its potential risks. There is no need for AI-specific legislation for now, as existing laws can cover its use and regulators will issue guidelines to organisations so that they have a clearer picture of how to conduct their affairs.

However, the government will enact legislation if it is necessary to do so, and this will be done "thoughtfully and in concert with others, accounting for the global nature of AI" (NAIS 2.0). The approach is dependent on the nature of the risk to and from AI, where some cases are best settled by voluntary guidelines, and others by legislation.

3.2 Jurisdictional Law

Singapore's approach to AI so far has been to issue voluntary guidelines and guidance notes to aid industries in navigating this new technology and set out best practices. Guidelines are suitable for an area in which change is rapid, as they can be amended and issued quickly.

As mentioned in **1.1 General Legal Background**, Singapore has not yet enacted legislation that regulates the use of AI in general. However, there is legislation that concerns two specific applications of AI – namely, autonomous vehicles (AVs) (see **14.4 Autonomous Vehicles**) and AI-MDs (see **14.3 Healthcare**).

3.3 Jurisdictional Directives
Please refer to **1.1 General Legal Background** for the key jurisdictional directives.

3.4 EU Law
3.4.1 Jurisdictional Commonalities
This is not applicable in Singapore.

3.4.2 Jurisdictional Conflicts
This is not applicable in Singapore.

3.5 US State Law
This is not applicable in Singapore.

3.6 Data, Information or Content Laws
In relation to personal data that is used to train AI systems or that is processed by AI systems, Singapore's Personal Data Protection Act 2012 (for private sector data) will apply, as it is technology-agnostic. The PDPC has also issued its first PDPC AI Advisory Guidelines to set out best practices for organisations developing or deploying AI systems. For more details, please refer to **11.2 Data Protection and Privacy**.

In relation to copyright issues arising from the use of data to train AI systems, Singapore has a computational data analysis exception under Section 244 of the Copyright Act 2021, which was introduced after a public consultation in 2019. This is independent of the fair use exception under Section 190 of the Copyright Act 2021. For more details, please refer to **8.2 IP and Generative AI**.

3.7 Proposed AI-Specific Legislation and Regulations
There is no AI-specific legislation that is pending enactment in Singapore at present – although this is not something that the authorities are closed-off to, as set out in the NAIS 2.0. Please refer to **3.1 General Approach to AI-Specific Legislation**.

4. Judicial Decisions

4.1 Judicial Decisions
Singapore's Court of Appeal has issued a key decision on the use of deterministic algorithms in contracting. Singapore does not yet have reported decisions on the use of AI and the surrounding IP rights.

In Quoine Pte Ltd v B2C2 Ltd (2020) SGCA(I) 02 ("Quoine"), transactions on Quoine's cryptocurrency exchange platform were conducted by algorithms for both Quoine and B2C2, with the algorithms giving trading instructions based on observations of market data. Owing to an oversight, Quoine failed to make certain changes to several critical operating systems on its platform, so it could not generate new orders. It is relevant that B2C2 had – back when designing its algorithm – set a virtual price of 10 Bitcoin to 1 Ethereum in the event that there was insufficient market data from Quoine to draw upon in order to price its trades.

Quoine's oversight sparked off a chain of events that triggered buy orders for Ethereum being placed on behalf of some platform users – at 250 times the going market rate for purchasing Ethereum with Bitcoin – in favour of B2C2. This was the virtual price B2C2 had set to sell its Ethereum.

Quoine cancelled the trades when it realised this and B2C2 sued Quoine as a result. Quoine argued that the contracts were void/voidable for unilateral mistake. It is important to note that all the algorithms functioned as they should and that the cause was actually human error.

The court described a deterministic algorithm as one that "will always produce precisely the same output given the same input", where it "will do just what it was programmed to do and does not have the capacity to develop its own responses to varying conditions" and "hence, faced with any given set of conditions, it will always respond to that in the same way" (at (15)).

The court held that where contracts are made by way of deterministic algorithms, in order to determine knowledge, the court would refer to the state of mind of the algorithm's programmers from the time of the programming up to the point that the relevant contract is formed (see (97) to (99)). The court upheld the contract, as it found that the programmer did not have actual or constructive knowledge of Quoine's mistake, and hence did not unconscionably take advantage of it.

It would be interesting to see whether the same principles would apply in the case of a non-deterministic algorithm, as the outcome may not always be known and the computer could be said to "have a mind of its own" (see (185)), or if there are multiple programmers – given that, in Quoine, the software used by B2C2 was devised almost exclusively by one of the founders.

4.2 Technology Definitions

Although the concept of a "deterministic algorithm" was explored in Quoine (see **4.1 Judicial Decisions**), AI was not defined in the case.

5. AI Regulatory Oversight

5.1 Regulatory Agencies

All ministries and statutory boards have a part to play in developing Singapore's use of AI. The following is a non-exhaustive list of key regulatory agencies.

- The Smart Nation and Digital Government Office (SNDGO) is under the Prime Minister's Office, where it plans and prioritises key national projects and drives the digital transformation of the government. The SNDGO issued the National AI Strategies.
- The Government Technology Agency ("GovTech") is the implementing arm of the SNDGO, in which it develops products for the public and government, in addition to managing cybersecurity for the government.
- The IMDA regulates the infocommunications and media sectors and drives Singapore's digital transformation. The PDPC is part of the IMDA, where it implements policies to balance the protection of an individual's personal data with organisations' need to use it.
- The IPOS has initiated fast-track programmes for patent protection and copyright protection to support AI innovation.

Other bodies have also been set up that will complement the work of the regulatory agencies.

- The Advisory Council on the Ethical Use of AI and Data – chaired by the former Attorney-General V K Rajah SC and comprising 11 members from diverse industry backgrounds (multinational corporations and local companies, as well as advocates of social and consumer interests) – works with the government on responsible development and deployment of AI, advising on ethical, policy and governance issues.
- AI Singapore, a national programme comprising a partnership between various economic agencies (eg, the IMDA, Enterprise Singapore, and the SNDGO) and academia, was

launched in May 2017 to accelerate AI adoption by industry.
- The AI Verify Foundation, a non-profit that is a wholly owned subsidiary of the IMDA, was launched in June 2023 to create a global open source community to contribute to the use and development of AI testing frameworks, code base, standards and best practices. It has more than 100 corporate members ranging from multinational technology companies to banks to e-commerce companies.

5.2 Technology Definitions

The Model Framework (covering traditional AI) defines AI as "a set of technologies that seek to simulate human traits (such as knowledge, reasoning, problem-solving, perception, learning and planning) and, depending on the AI model, produce an output or decision (such as a prediction, recommendation and/or classification)". The authors have included this definition because the Model Framework applies across all sectors.

The Model Gen-AI Framework defines generative AI as "AI models capable of generating text, images or other media", which "learn the patterns and structure of their input training data and generate new data with similar characteristics".

Other documents issued by regulatory agencies also define "artificial intelligence", "machine learning", etc. Singapore's regulatory agencies take a co-ordinated approach towards AI; therefore, if there are any differences in definition across their documents, it will be due to the context in which the term appears.

5.3 Regulatory Objectives

Generally, all regulatory agencies seek to build public trust in the use of AI in Singapore and minimise the risks posed by AI, including traditional safety risks (such as injury and property damage), loss of privacy, bias, and other ethical concerns. They do this by ensuring that:

- the decision-making process is explainable, transparent and fair when AI is used to make decisions;
- AI solutions are human-centric (ie, promote the well-being and safety of humans); and
- there is accountability for all players in the AI development chain so that they are responsible towards end users.

5.4 Enforcement Actions

There is presently no reported enforcement action by regulators concerning the use of AI.

6. Standard-Setting Bodies

6.1 National Standard-Setting Bodies

Enterprise Singapore oversees the setting of standards in Singapore through the industry-led Singapore Standards Council.

On 31 January 2019, Enterprise Singapore published a Technical Reference for Autonomous Vehicles, known as "TR 68". This was born out of a year-long industry-led effort administered by the SSC's Manufacturing Standards Committee. The TR 68 was intended to set a provisional national standard to guide the industry in the development of fully autonomous vehicles. In 2021, following a review by the Land Transport Authority and the SSC, TR 68 was updated to include guidelines on the application of machine learning, software updates management, cybersecurity principles and testing framework.

The SSC has also published TR 99:2021, which provides guidance for assessing and defending against AI security threats.

6.2 International Standard-Setting Bodies

Singapore actively participates in standard-setting and norm-shaping processes with key international organisations and standard-setting organisations such as the World Economic Forum, the OECD, the International Organisation for Standardisation (ISO), and the International Electrotechnical Commission (IEC).

AI Singapore (see **5.1 Regulatory Agencies**) also actively participates in international standards bodies. In 2019, the AI Technical Committee (AITC) was formed to recommend the adoption of international AI standards for Singapore and support the development of new AI standards. The AITC represents Singapore as a participating member in ISO/IEC JTC 1/SC 42 – the international standards committee responsible for standardisation in the area of AI. To date, the AITC has contributed to the development and publication of two standards:

- ISO/IEC TR 24030:2021 Information Technology – Artificial Intelligence (AI) – Use Cases; and
- Singapore Standards TR 99:2021 Artificial Intelligence (AI) security – Guidance for assessing and defending against AI security threats.

7. Government Use of AI

7.1 Government Use of AI

Across the Singapore government, AI solutions are being adopted, including the following.

- The MAS is using machine learning models to analyse market trading data in order to identify potential instances of market collusion or manipulation for further investigations.
- The Singapore Police Force (SPF) is using AI to sieve out material that is likely to be obscene from seized devices to improve the efficiency of investigations.
- The SPF also partnered with the National Crime Prevention Council and GovTech to combat scams through the development of the "Scamshield" application, which uses AI to filter scam messages through the identification of keywords and blocks calls from blacklisted numbers.
- The Land Transport Authority (LTA) uses video analytics and AI to maintain more than 9,500 kilometres of roads more efficiently, thereby saving up to 30% of man-hours needed for detecting road defects. The LTA uses high-speed cameras mounted onto a van to automatically detect and report road defects, which enables targeted and predictive maintenance of roads.

In February 2023, the government announced a pilot project known as "Pair" that integrates ChatGPT into Microsoft Word to assist public officers in their writing and research. Agreements were made to ensure that confidential information would not be available Microsoft and OpenAI. Work that contains highly confidential or sensitive information will also continue to be written exclusively by civil servants as an additional safeguard.

7.2 Judicial Decisions

The Singapore courts are unlikely to use AI tools – eg, tools that assess an offender's risk of recidivism or recommend a sentence – for sentencing within the foreseeable future. The Chief Justice stated at the Sentencing Conference held on

31 October 2022 that the underlying algorithms for such systems were opaque and the data and assumptions that they are built upon could reflect bias. Instead, for greater consistency in sentencing, Singapore will have a Sentencing Advisory Panel that will issue publicly available sentencing guidelines that are persuasive but not binding on the courts.

However, the Singapore courts will use AI to improve access to justice. In September 2023, they signed a memorandum of understanding with Harvey AI, an American start-up, to trial its technology to assist litigants-in-person at the small claims tribunal. The goal is for the AI to give the litigant information on their next steps and what material they need to submit to support their claim.

7.3 National Security

The Ministry of Defence and the Singapore Armed Forces (SAF) have been exploring the use of AI in military operations to enhance capabilities and stay ahead of potential security threats. One such example is the upgraded command and control information system that helps commanders make faster decisions through displaying a real-time battlefield picture integrated with the best options commanders can take to neutralise the threat.

AI is also being used to enhance the safety of servicemen during training and operations. The SAF Enterprise Safety Information System leverages data science and AI technologies to identify potential risks in operations and recommend pre-emptive action to prevent potential accidents. Additionally, in order to better utilise manpower, the SAF is also conducting trials on the use of AVs in military camps for the unmanned transportation of supplies and personnel.

8. Generative AI

8.1 Emerging Issues in Generative AI

For the discussion of IP issues, see **8.2 IP on Generative AI**, and for data protection issues, see **8.3 Data Protection and Generative AI**.

8.2 IP and Generative AI

There are three key IP issues arising from the use of generative AI.

Use of Copyrighted Content to Train a Generative AI System

There are no cases brought before the Singapore courts yet. Lawsuits have been filed overseas against LLM providers and text-to-image providers, and the outcomes of these lawsuits will be relevant to Singapore.

In Singapore, under Section 244 of the Copyright Act 2021, making a copy of any copyrighted work is permissible if it is for the purpose of computational data analysis (as defined in Section 243 of the Copyright Act 2021 – eg, using images to train a computer program to recognise images) or preparing the work for computational data analysis, provided that certain conditions are met. Singapore also has the fair use exception under Section 190 of the Copyright Act 2021. Both Sections 190 and 244 of the Copyright Act 2021 have not yet been tested in Singapore courts in the context of training generative AI systems.

Protection of the Output of the Generative AI System Under Copyright and/or Patent Laws

This is a developing area of law both overseas and in Singapore. A report ("When Code Creates: A Landscape Report on Issues at the Intersection of Artificial Intelligence and Intellectual Property Law"), published on 28 February 2024 by IPOS and the Singapore Management Uni-

versity, highlights that there is a spectrum of AI involvement and draws a distinction between "AI-generated" inventions and works (ie, no human intervention) and "AI-assisted" inventions and works (ie, where AI is used as a tool like a paintbrush).

In relation to copyright, the current position under the Copyright Act 2021 is that the author must be a natural person. Hence, whether copyright can subsist in the output of generative AI is likely to depend on two factors:

- the extent to which the human involved in prompting the generative AI exercised creativity in the prompting process and the subsequent editing of the output; and
- the nature of the output of the generative AI (as not all works are by their nature protected by copyright).

In relation to patents, the "inventor" must also be a natural person under Singapore law. As with copyright, the output may be protected depending on the level of involvement of the human who prompted the generative AI.

Liability for Copyright Infringement Resulting from the Output of Generative AI

This is also a developing area of law in Singapore and around the world. Whether or not the use of generative AI's output can result in a person being liable for copyright infringement if the output is substantially similar to an existing work depends in part on how the Generative AI works – ie, how it is trained and how it produces its output. LLMs such as ChatGPT, for example, generate text based on the statistical probability of one word appearing after another and this may suffice as an explanation for the similarities in the works – although cases running this defence are still making their way through the courts.

In theory, AI image generators also create a new image based on the text prompt received – albeit not by replicating an existing image (or part of it) that it has been trained on. Instead, AI image generators produce their own image based on their own "understanding" of what the "essence" of an object is after being trained on tens of thousands of photographs of the object.

For more details on IP protection of an AI system itself (and not its output), please see **15.1 Applicability of Patent and Copyright Law** and **16.2 Applicability of Trade Secret and Similar Protection**.

8.3 Data Protection and Generative AI

The Personal Data Protection Act 2012 (PDPA) applies to the collection, use and disclosure of personal data by organisations. Organisations may only collect, use and disclose personal data "for purposes that a reasonable person would consider appropriate in the circumstances" (Section 3). For the legal bases for the collection, use and disclosure of personal data (eg, consent and other bases), please see **11.2 Data Protection and Privacy**.

A data subject has the right to access their personal data held by an organisation (Section 21; subject to certain exceptions), as well as request that an organisation corrects an error or omission in the personal data about them that is in the possession or under the control of the organisation (Section 22; subject to certain exceptions). At the same time, an organisation also has a duty to "make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data is likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates" (Section 23).

However, when it comes to the output of generative AI, which may make false factual claims about an individual, there are no reported cases locally yet. Regulators are working to address the risk of "hallucinations" (whereby false information is given by a generative AI system) and the Model Gen-AI Framework recommends techniques such as Retrieval-Augmented Generation and few-shot learning to reduce hallucinations and improve the accuracy of output.

It remains to be seen if courts or regulators in Singapore will order deletion of the entire AI model or cease the use of such AI model if it is trained on illegally obtained personal data. However, given that there have been reported instances of this in other jurisdictions, the authors cannot rule out such a response locally if the situation warrants it.

9. Legal Tech

9.1 AI in the Legal Profession and Ethical Considerations

Law firms in Singapore are using AI for document review, for due diligence processes in M&A transactions, and to summarise contractual documents – to name just a few uses.

Singapore's Chief Justice Sundaresh Menon has shared his views (at the Litigation Conference held on 3 April 2024) on how AI will reshape the legal profession: automation of routine legal tasks will reduce the demand for junior lawyers and paralegals, but at the same time increase the demand for legally trained persons with an expertise in technology to develop AI tools for legal work. The legal profession will have to learn and adapt to using such AI tools – for example, how to engineer prompts for the AI system to produce the most relevant and useful output. Legal professionals must also uphold their professional responsibilities when using AI tools, such as by verifying the accuracy of AI-generated output and ensuring that confidential client information is not included in prompts to public generative AI tools.

10. Liability for AI

10.1 Theories of Liability

Where the use of AI gives rise to personal injury, property damage or financial loss, the claimant can seek a remedy in tort (negligence) or contract. Singapore does not have product liability laws like those in the UK or the EU. Instead, remedies are available under statutes such as the Unfair Contract Terms Act 1977 and the Sale of Goods Act 1979, as well as specific legislation (eg, the HPA) and the common law (contract and tort).

Singapore has not amended its laws to provide for any special rules concerning liability arising from the use of AI. As yet, there have been no cases in court involving damages due to AI not performing as expected.

The authors are of the view that there are three features of AI that may affect the application of conventional principles of liability, as follows.

- AI is a "black box" – it is not always possible to explain how or why an AI system reached a particular outcome and the type of model chosen affects how easily its workings can be explained.
- AI is self-learning/autonomous – it has the ability to learn from the data it has been exposed to during its training and improve without being explicitly programmed, mean-

ing the behaviour of the AI system is not always foreseeable.
- AI has many people involved in its development – from procuring the datasets, to training the algorithm, to selecting the algorithm, to monitoring the performance of the algorithm. So who is to blame when the AI output is not as expected or if it causes harm?

Fault-Based Liability (Negligence)

Negligence requires that someone owes a duty of care, that there is breach of such duty (falling below the standard of care), and that the breach caused the loss. Owing to the nature of AI, where many people are involved in its development, the plaintiff might find it difficult to identify the party at fault and the identified party could try to push the blame to a party upstream or downstream in the AI life cycle. However, the Model Gen-AI Framework suggests that liability could be allocated based on the level of control that each stakeholder has in the AI development chain.

Next comes the requirement to prove breach of the standard of care. However, if the opacity of AI makes it impossible to explain why it reached an outcome, then it may be difficult to prove that the behaviour of the AI was due to a defect in the code (rather than any other reason). As the use of AI is developing, it is not clear what standard of care will apply either. Furthermore, even where there is a human in the loop to review the outcome of the AI system, the human will not be able to determine whether the AI is making an error in time to prevent it if the AI is meant to exceed human capabilities.

Finally, there is a requirement to show that the breach caused the loss. Even though it could be argued that the autonomous nature of AI breaks the chain of causation, such an argument is unlikely to be accepted on public policy grounds. In contrast with the EU's new AI Liability Directive, Singapore has not introduced any laws that introduce a rebuttable presumption of causality between the defendant's fault and the damage resulting from the AI system's output (or failure to produce one).

Contract Liability

With a contract, parties negotiate to pre-allocate the risk, so this may resolve some of the issues faced in tort of who is the responsible party. However, establishing whether there is a breach will depend on what parties have agreed to in the contract – for example, whether there are specific, measurable standards the AI system must meet. The Sale of Goods Act 1979 (which provides for an implied condition that goods supplied under the contract are of satisfactory quality) will only apply to the extent that the AI system is a good if it is not embedded in hardware such as a physical disc.

Liability Independent of Fault (Strict Liability/ Product Liability)

As mentioned previously, Singapore does not have product liability laws like those in the UK/EU. Nevertheless, the Singapore Academy of Law's Law Reform Committee considered the application of those laws in its Report on the Attribution of Civil Liability for Accidents Involving Autonomous Cars (published September 2020) and found that product liability presents the same difficulties as negligence because the claimant generally still has to show some fault on the manufacturer's part (ie, prove there is a "defect" with the software) (see (5.17)–(5.18) of the Report).

Whether there will be strict liability imposed for damage arising from the use of AI remains to be seen, as policymakers must strike a balance

between ensuring that innovation is not stifled and obtaining a remedy with ease.

10.2 Regulatory

At present, there are no proposed regulations regarding the imposition and allocation of liability for the use of AI.

The Singapore Academy of Law's Law Reform Committee has issued two reports that make recommendations on the application of the law to robotic and AI systems in Singapore, namely:

- Criminal Liability, Robotics and AI Systems (February 2021); and
- The Attribution of Civil Liability for Accidents Involving Autonomous Cars (September 2020).

11. Legal Issues With Predictive and Generative AI

11.1 Algorithmic Bias

The Model Framework highlights the risk of "bias" in the data used to train the AI model and proposes some solutions to minimise it. The IMDA/PDPC acknowledge the reality that virtually no dataset is completely unbiased; however, where organisations are aware of this possibility, it is more likely that they can take steps to mitigate it. Organisations are encouraged to collect data from a variety of reliable sources and to ensure that the dataset is as complete as possible. It is noted that premature removal of data attributes may make it difficult to identify inherent biases in the data.

In addition, the model should be tested on different demographic groups to see if any groups are being systematically advantaged or disadvantaged. Running through the questions in the ISAGO or AI Verify will also help organisations to reduce bias in the AI development process. In relation to LLMs, the IMDA's October 2023 paper on "Cataloguing LLM Evaluations" sets out recommended evaluation and testing approaches for bias.

There have not been any reported regulatory actions or judicial decisions with regard to algorithmic bias in Singapore.

11.2 Data Protection and Privacy

The collection, use and disclosure of personal data in Singapore is subject to the PDPA. The PDPC has also issued its AI Advisory Guidelines in March 2024.

Legal Bases for the Collection, Use or Disclosure of Personal Data

The use of AI to process personal data is prevalent because AI can generate many useful insights from data. However, regardless of whether AI technology is used in relation to the data, there first and foremost must be a legal basis for the collection, use or disclosure of personal data.

Consent is one of the bases but has its limitations, including an individual's right to withdraw consent to their data being used or the requirement to notify the individual of a new purpose for the use of their personal data if no such consent was sought before.

Therefore, other relevant bases for the collection, use or disclosure of personal data are:

- general legitimate purposes, provided that certain conditions are met, such as:
  - (a) identifying and articulating the legitimate interest;
  - (b) conducting a data protection impact as-

sessment; and
(c) disclosing to the individual reliance on the legitimate interests exception;
- for the purpose of entering, managing or terminating an employment relationship with an individual, provided that the individual is notified of the purposes of such collection, use or disclosure; and
- business improvement purposes – for example, improving and enhancing any goods or services provided, or developing new goods or services, or learning or understanding the behaviour and preferences of individuals in relation to providing goods and services – provided certain conditions are met, such as:
  (a) the organisation is of the view that the purposes cannot reasonably be achieved without using the personal data in an individually identifiable form; and
  (b) the purpose would be considered appropriate in the circumstances by a reasonable person.

Anonymised Data

The PDPC encourages organisations to use anonymised data when developing, testing and monitoring AI systems as much as possible. Anonymised data is not considered personal data for the purposes of the PDPA. However, there is always a risk of re-identification in combination with other data about the individual – especially where AI makes connections between different datasets and creates a profile about the person, whereby the data that is anonymised now becomes personal data subject to the PDPA.

11.3 Facial Recognition and Biometrics

Generally, biometric data such as fingerprints and likeness – when associated with other information about an individual – will form personal data under the PDPA. As such, any organisation that collects, uses or discloses such data will be subject to the obligations under the PDPA.

The PDPC has released the Guide on Responsible Use of Biometric Data in Security Applications. This guide specifically addresses the use of biometric data in relation to security cameras and CCTVs for security monitoring and facial or fingerprint recognition systems for security purposes to control movement in and out of premises. It highlights certain risks of using such data and measures that organisations may implement to mitigate the risks.

First, there is a risk of identity spoofing where a synthetic object (such as a 3D mask) is used to fake the physical characteristics of the individual in order to obtain a positive match in the system. Organisations should thus consider implementing anti-spoofing measures such as liveliness detection or installing such biometric systems near a manned security post.

Second, there is a risk of error in identification through false negatives or false positives. This may occur when the threshold for matching is set either too high or too low and the system fails or wrongly identifies a person. Organisations should thus implement a reasonable matching threshold, taking into account industry practice, and/or have additional factors of authentication to complement the existing matching thresholds.

Finally, there are systemic risks to biometric templates where the uniqueness of a biometric template may be diluted (and thus vulnerable to adversaries) if the algorithm used to create the template is used multiple times by the service provider across different sets of customers. Organisations should consider encrypting the biometric template in the database or use customised algorithms.

11.4 Automated Decision-Making

The Model Framework encourages organisations to consider the appropriate level of human oversight in AI-augmented decision-making. Broadly speaking, there are three degrees of human oversight:

- human-in-the-loop – the human is in full control and the AI only provides a recommendation;
- human-out-of-the loop – there is no human oversight and the AI is in full control; and
- human-over-the-loop – the human is monitoring or supervising the output and can take control in the event of unexpected or unusual cases.

In determining the level of human involvement required, the Model Framework sets out the following factors:

- probability of the harm occurring (high/low);
- severity of the harm occurring (high/low) – for example, the impact of wrong medical diagnosis compared with the consequences of shopping recommendations;
- nature of the harm (whether physical or intangible in nature);
- reversibility of the harm, including the avenues for recourse of the individual; and
- whether it is feasible or meaningful for a human to be involved at all (human involvement is not feasible in high-speed financial trading as per the case of Quoine).

Lastly, the Model Framework encourages organisations to disclose their use of AI so that persons are aware that they are interacting with it and, in particular, to:

- explain how AI is used in the decision-making process and what factors are taken into account in making the decision;
- offer an option to opt out from the use of AI, if it is feasible to so; and
- allow affected persons to appeal against an AI decision that materially affects them – the person should be given enough information about the reasons for the previous decision so that the person can effectively craft their appeal.

11.5 Transparency

To build trust in the use of AI, the Model Framework encourages organisations to ensure that consumers are aware that they are interacting with AI (whether in the case of chatbots or other technologies that are a substitute for services rendered by natural persons). For more details on disclosures, see **11.4 Automated Decision-Making**.

Singapore has also stated (in the ASEAN Guide on AI Governance and Ethics) that AI systems should not be used to manipulate consumer behaviour – namely, that "AI systems should not be used for malicious purposes or to sway or deceive users into making decisions that are not beneficial to them or society".

11.6 Anti-competitive Conduct

Pricing algorithms range from those that monitor and extrapolate trends in prices in the market to those that can weigh information such as supply and demand, customer profile and competitor's pricing in order to make real-time adjustment to prices. Such algorithms raise three key issues of concern when it comes to competition law.

Algorithmic Collusion

The individual use of a pricing algorithm does not fall foul of competition law. However, where

organisations have an explicit agreement to collude and use pricing software to implement their agreement, the Competition and Consumer Commission of Singapore (CCCS) has unequivocally stated that this will contravene Section 34 of the Competition Act 2004 as an agreement that prevents, restricts or distorts competition.

If organisations use a distinct algorithm with no prior or ongoing communication, but achieve an alignment of market behaviour, the CCCS will take a fact-centric approach to determine whether the collusive outcomes can be attributed to the organisations.

Personalised Pricing

Where an organisation with a dominant position in the market utilises AI to implement personalised pricing, it may be deemed an exclusionary abuse of dominance and infringe Section 47 of the Competition Act 2004. Specifically, if personalised pricing is used to set discounts that foreclose all or a substantial part of a market, the CCCS may find that the organisation has abused its dominance in the market.

Liability Where AI Learns Collusive Behaviour

If an AI system autonomously learns and implements collusive behaviour, the CCCS is unlikely to find no fault on the part of the organisation that deploys the AI system. Although it is non-binding, the Model Framework states that organisations should be able to explain decisions made by AI. Accordingly, organisations are unlikely to be able to disclaim responsibility for the decisions made by the AI they deploy.

12. AI Procurement

12.1 Procurement of AI Technology

The ASEAN Guide on AI Governance and Ethics recommends that deployers who procure AI systems from third-party developers should "appropriately govern their relationships with these developers through contracts that allocate liability in a manner agreed between parties". The deployer should also require the developer to assist it in meeting its transparency and explainability obligations to both customers and regulators. The ASEAN Guide on AI Governance and Ethics also recommends that deployers and developers collaborate to conduct joint audits and assessments of the AI system, and testing frameworks such as Singapore's AI Verify may be used for this purpose.

13. AI in Employment

13.1 Hiring and Termination Practices

AI can be used to screen CVs and identify select candidates to move to the next round, thereby making the hiring process more efficient. However, an AI system is only as good as the humans who programmed it, and it is also susceptible to biases in the data it is trained on – for example, the training data may be weighted heavily in favour of one gender for a role.

The Tripartite Guidelines on Fair Employment Practices set out fair employment practices for employers to abide by. Employees must be selected on the basis of merit (ie, skills and experience), regardless of their age, race, gender, religion, marital status and family responsibilities, or disability. Therefore, automated employment screening tools must not take into account such characteristics (with the exception of gender where it is a practical requirement of

the job – for example, hiring a female masseuse to do spa treatments for female customers).

The Ministry of Manpower can take action against employers who do not follow the Tripartite Guidelines by curtailing their work pass privileges, such that they may not apply for new work passes or renew the work passes of their existing employees. Singapore intends to introduce workplace fairness legislation in the second half of 2024, so as to complement the existing Tripartite Guidelines.

13.2 Employee Evaluation and Monitoring

Although organisations will require consent to collect, use or disclose such personal data, organisations may also rely on two exceptions under the PDPA to do so without obtaining consent from the individual. However, the organisation must still act based on what a reasonable person considers appropriate in the circumstances — it does not have carte blanche to collect every single piece of personal data about an employee through its employee monitoring software. This is because the employer's monitoring of the employee's email account, internet browsing history, etc, can reveal very private information about the employee, including private medical information that may not be relevant to the employee's workplace performance.

The first exception is where the collection, use or disclosure of personal data is for the purpose of managing or terminating an employment relationship between the organisation and the individual. However, to rely on this exception, the organisation must inform its employees of the purposes of such collection, use or disclosure – for example, through the employment contract or employee handbooks. The second exception is where the collection, use or disclosure of personal data about an individual is necessary for evaluative purposes (ie, for determining the suitability or eligibility of the individual for employment, promotion, or continuance in employment).

Although consent may not be needed to collect such data, organisations should be aware that other obligations under the PDPA – for example, the protection obligation to prevent unauthorised access to the data – continue to apply.

14. AI in Industry Sectors

14.1 Digital Platform Companies

A Parliamentary question of 12 September 2022 concerned whether the government will:

- consider regulating platform companies to ensure they do not encourage excessive risk-taking (eg, taking on too many jobs in an hour or riding during dangerous weather) by the workers to fulfil orders; and
- study the AI and algorithms of such companies to ensure this is not the case.

The Ministry of Manpower (MOM) responded that it will be "cautious" about regulating the incentives and algorithms of such companies. The MOM would resolve the issue through discussions with tripartite partners and strengthening protections for workers, "rather than jump to regulation and risk over-regulation".

The government has since accepted the recommendations of the Advisory Committee on Platform Workers in November 2022, thereby strengthening protections for platform workers in terms of financial protection in case of work injury, improving housing and retirement adequacy, and enhancing representation for such workers.

A legislative framework and other policies will be introduced in the second half of 2024.

14.2 Financial Services

Firms that use AI and data analytics to offer financial products and services should reference the Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector, which was published by the MAS in 2018. The principles align with the Model Framework and are voluntary; financial services companies must continue to comply with all other applicable laws and requirements.

The MAS also leads an industry consortium ("Veritas") that creates frameworks for financial institutions to assess their use of Artificial Intelligence and Data Analytics (AIDA) solutions against the FEAT principles. The White Papers arising from each phase of Veritas (there have been three phases to date since 2019) are published on the MAS website.

Digital advisers (or robo-advisers) are automated, algorithm-based tools with limited or no human adviser interaction. Where such tools are used to provide advice on investment products, the MAS Guidelines on Provision of Digital Advisory Services state that they should minimally provide the client with the following information:

- assumptions, limitations and risks of the algorithms;
- circumstances under which the digital advisers may override the algorithms or temporarily halt the digital advisory service; and
- any material adjustments to the algorithms.

14.3 Healthcare

As mentioned in **1.1 General Legal Background**, the HPA requires medical devices to be registered. AI-MDs are a type of "medical device" (as defined in the HPA) – hence they must be registered – and they are subject to further requirements for registration by the HSA's Regulatory Guidelines for Software Medical Devices. Under those Guidelines, additional information must be submitted when registering the AI-MD – for example, information on the datasets used for training and testing and a description of the machine-learning model that is used in the AI-MD.

However, when it comes to liability for errors made by an AI-MD or by any other AI application, there are no judicial decisions yet as to who is liable (or jointly liable) for the error – ie, whether the hospital, doctor, developer of the AI system, etc, is liable.

14.4 Autonomous Vehicles

Singapore's Road Traffic Act 1961 provides a regulatory sandbox for the use and testing of AVs – see Sections 2(1), 6C, 6D and 6E, and the Road Traffic (Autonomous Motor Vehicles) Rules 2017 ("the Rules"). The Rules prohibit the trial or use of an AV without authorisation and, among other things, set out:

- the application process for authorisation;
- the conditions of authorisation (eg, requiring a qualified safety driver to be seated in the AV to monitor its operation and take over if necessary);
- that a data recorder must be installed in the AV;
- that there must be liability insurance or security in lieu of liability insurance; and

- that any incident or accident involving the AV must be reported to the Land Transport Authority.

When asked about liability for AV accidents in 2017, the then-Second Minister for Transport responded: "The traditional basis of claims for negligence may not work so well where there is no driver in control of a vehicle. When presented with novel technologies, courts often try to draw analogies to legal constructs in other existing technologies. In the case of AVs, the courts have autopilot systems for airplanes, autopilot navigational systems for maritime vessels, and product liability law to draw references from. As with accidents involving human-driven vehicles, it is likely that issues of liability for AVs will be resolved through proof of fault and existing common law."

14.5 Manufacturing

Please see **10.1 Theories of Liability**, which sets out potential remedies when AI systems do not function as intended or cause harm.

14.6 Professional Services

Please see **9.1 AI in the Legal Profession and Ethical Considerations**, where the issues across professional services are similar. Professionals must be mindful of the risks and limitations of AI and take steps to verify the accuracy of the output, critically analyse it for bias, and ensure that confidential client data is not input into an AI system where it can be accessed by unauthorised third parties.

In terms of liability, a person cannot delegate their professional responsibility (eg, a duty to provide correct information) to an AI system. Hence, if they were to rely on the output of an AI system, they would ultimately remain responsible for it.

15. Intellectual Property

15.1 Applicability of Patent and Copyright Law

Protecting AI Innovations Through Patent

Under Section 13 of the Patents Act 1994, an invention must fulfil the following three conditions to be patentable:

- the invention must be new;
- the invention must involve an inventive step; and
- the invention must be capable of industrial application.

However, not all inventions are eligible for patent protection (even if they meet the three conditions). The Examination Guidelines for Patent Applications of the IPOS are instructive. Neural networks, support vector machines, discriminant analysis, decision trees, k-means and other such computational models and algorithms applied in machine learning are mathematical methods in themselves and are thus not considered to be inventions by the IPOS.

However, where the claimed subject matter relates to the application of a machine-learning method to solve a specific (as opposed to a generic) problem, this could be regarded as an invention because the actual contribution of the claimed subject matter goes beyond the underlying mathematical method. Solving a generic problem by using the method to control a system, for example, is unlikely to cross the threshold. The application must be a specific one, such as using the method to control the navigation of an AV.

Protecting AI Innovations Through Copyright

Source codes and AI algorithms are protected by copyright.

Protecting Output Generated by AI

The extent to which copyright and/or patent laws protect the output of generative AI systems is discussed in **8.2 IP and Generative AI**.

15.2 Applicability of Trade Secrecy and Similar Protection

AI innovations may also be protected under the law of confidence, as set out in the IPOS' IP and Artificial Intelligence Information Note. Generally, confidential information refers to non-trivial, technical, commercial or personal information that is not known to the public, whereas trade secrets usually describe such information with commercial value.

Information will possess the quality of confidence if it remains relatively secret or inaccessible to the public in comparison with information already in the public domain. Therefore, it is important to secure the confidential information by implementing non-disclosure agreements, encrypting materials, and classifying information so as to limit access to only select groups of people.

However, it is not possible to protect an AI innovation under both patent and the law of confidence because the former requires public disclosure, which destroys the quality of confidence. Therefore, when deciding which regime to use to protect their work, AI innovators should consider whether the invention constitutes patentable subject matter and if the invention is likely to be made public soon or can be easily derived by others through reverse engineering.

15.3 AI-Generated Works of Art and Works of Authorship

See the issues outlined in **8.2 IP and Generative AI**.

15.4 OpenAI

See the issues outlined in **8.2 IP and Generative AI**.

16. Advising Corporate Boards of Directors

16.1 Advising Directors

When deploying AI solutions, an organisation should adopt the good governance measures set out by the Model Framework in the following four key areas.

Internal Governance Structures and Measures

All personnel involved in the development of an AI solution should have clear roles and responsibilities, as well as sufficient expertise, resources and training to discharge their duties. A co-ordinating body should be drawn from across the organisation if necessary. The organisation should also establish a monitoring and reporting system to ensure that the appropriate level of management is aware of the performance of the AI solution.

Determining the Level of Human Involvement in AI-Augmented Decision-Making

The level of human oversight in AI-augmented decision-making will depend on how the balance is struck between the commercial objectives/advantages of using AI and the risks of using AI. For more details, please see **11.4 Automated Decision-Making**.

Operations Management

As the effectiveness of an AI system is dependent on the data it is trained on, good data accountability practices should be implemented – such as understanding the lineage of the data used, ensuring its accuracy, minimising any inherent

bias in the datasets, and periodically reviewing and updating the datasets.

The organisation also needs to document the process of creating the AI system, from the reasons behind decisions such as choosing the datasets for training the model (and why a particular model was selected) to the measures taken to address identified risks. In the event the AI system does not perform as expected, the organisation can then look back on its records to troubleshoot and also defend against liability.

Stakeholder Interaction and Communication

The organisation should consider how to build consumers' trust in its use of AI. Such steps would include disclosing the use of AI in the product/service provided, explaining its benefits and risks to the consumer, and maintaining open channels of communication for consumers to raise feedback/queries or apply for a review of a decision made by the AI system.

17. AI Compliance

17.1 AI Best Practice Compliance Strategies

With the abundance of AI guidelines and frameworks introduced across jurisdictions, it can be difficult for organisations to pick one to start with, especially if they intend to deploy their AI solution across multiple jurisdictions. Nevertheless, it is good to take one framework as a starting point or baseline and make improvements/adjustments from there, incorporating recommended actions from other jurisdictions that may not be found locally. Singapore's ISAGO is useful for both developers and deployers of AI solutions (albeit more for deployers), and it is broadly aligned to the AI governance frameworks in key AI jurisdictions. Organisations may also assess their systems with AI Verify (although the ISAGO is simpler, as it is a checklist with no technical tests).

Organisations should also create a generative AI use policy to set common expectations across employees on how they may use (or not use) generative AI tools such as ChatGPT. The policy can give examples of acceptable and unacceptable prompts for clarity.

Trends and Developments

Contributed by:
Lim Chong Kin and Cheryl Seah
Drew & Napier LLC

Drew & Napier LLC is a full-service Singapore law firm, which was founded in 1889 and remains one of the largest law firms in the country. Drew & Napier has a highly regarded TMT practice group, which consistently ranks as the leading TMT practice in Singapore. The firm possesses unparalleled transactional, licensing and regulatory experience in the areas of telecommunications, technology, media, data protection and cybersecurity. The TMT practice is supported by more than ten lawyers and paralegals with extensive experience in info-communications, data protection, technology, and sector-specific and general competition law. The TMT practice acts for a broad range of clients, spanning multinational corporations and local companies across industries. These clients include global and regional telecommunications service providers, sectoral regulators (both local and foreign), consultants, software houses, hardware manufacturers, and international law firms.

Authors

Lim Chong Kin is the managing director of Drew & Napier's corporate and finance department, head of the firm's TMT practice, and co-head of both its data protection, privacy and cybersecurity practice and its competition law and regulatory practice. With a strong background in competition, data protection and technology laws, he is often depended upon by clients to deliver commercially savvy advice, especially in the cutting-edge fintech and AI industries. Chong Kin has in-depth expertise and experience in competition law matters, in particular. Since 1999, he has advised the sectoral competition regulators on liberalisation matters, including drafting, implementing and enforcing the competition law framework for the telecommunications, media and postal sectors.

Cheryl Seah is a director of the corporate and finance department at Drew & Napier. Cheryl advises companies ranging from Fortune 500 multinational corporations to local and foreign start-ups on legal and governance issues at all stages of the AI life cycle – from procuring the computing resources, to the data used in model training, to the IP and liability issues arising from the output. She publishes frequently with the Law Society of Singapore on legal issues arising from the use of AI and has conducted talks on AI for external organisations (including a university) and regulators in South-East Asia. In her previous role in the Attorney-General's Chambers (Singapore's central law drafting office), she has drafted legislation across a wide variety of subjects, focusing on transport (including autonomous vehicles), infrastructure, technology and civil procedure.

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

Singapore's Approach to AI Adoption and AI Governance

Singapore has a highly supportive climate for the development and use of AI, both in terms of funding and policies. Singapore has also developed a comprehensive AI governance testing framework for traditional AI systems (AI Verify) and is working hard to ensure its AI governance frameworks are interoperable/aligned with the international community's. By way of example, Singapore actively participates in international fora and recently mapped the AI Verify framework to the USA's National Institute of Standards and Technology AI Risk Management Framework, declaring them interoperable (a mapping exercise with the EU will happen in the future). This will help organisations that offer AI systems in multiple markets, as the idea of interoperability is that if an organisation complies with country A's governance framework, it will also comply with country B's.

In relation to generative AI, which is a more recent development with the public release of ChatGPT in November 2022, Singapore released a draft Model AI Governance Framework for Generative AI (the "Model Gen-AI Framework") to seek public feedback internationally from 16 January to 15 March 2024, and has published the finalised version on 30 May 2024.

When it comes to regulating the use of AI, Singapore takes a measured approach, examining the use cases of AI first to see what risks arise that cannot be adequately addressed or mitigated by existing laws on areas such as data protection, IP protection and consumer protection. Singapore does not have legislation governing the general use of AI. However, it does have legislation in relation to AI-enabled medical devices, as medical devices (whether AI-enabled or not) are regulated under the Health Products Act 2007. Like most countries, Singapore also has legislation concerning the use/testing of autonomous vehicles (AVs) – given that its road traffic laws were premised on there being a human driver.

Nevertheless, in order to guide industries with regard to deploying AI, regulators in Singapore have issued guidelines for both traditional and generative AI, such as:

- the Model Artificial Intelligence Governance Framework (the "Model Framework"), which is a voluntary, sector-agnostic framework – issued by the Infocomm Media Development Authority (IMDA) and Personal Data Protection Commission (PDPC) – that sets out principles of AI governance, as well as practical methods by which they can be achieved (eg,

how to minimise bias in the datasets used for training);
- the Model Gen-AI Framework, setting out nine dimensions to build trustworthy generative AI, as well as the actions the industry and policymakers must take to achieve it;
- the Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector, issued by the Monetary Authority of Singapore (MAS); and
- the Artificial Intelligence in Healthcare Guidelines, which was issued by the Ministry of Health (MOH), the Health Sciences Authority (HSA) and the Integrated Health Information Systems in order to set out good practice for developers of AI in healthcare settings and complement the HSA's regulatory requirements for AI-enabled medical devices.

The strength of Singapore's approach to AI lies in its adaptability. Guidelines can be amended (or new guidelines issued) quickly to adapt to any changes. The technology, its use cases, and the issues arising from the use cases can be carefully studied before making any legislative changes that are more permanent in nature. Singapore also ensures that guidelines are formulated in close consultation with the industry, taking into account any feedback.

In the meantime, the IMDA and the PDPC are also working on testing methodologies in order to ensure that the use of AI is in line with the governance principles. This will also prevent Singapore enacting legislation that cannot be enforced.

Approaches to Regulating the Use of AI

With legislation and guidelines on the use of AI being issued across the world at such a rapid pace, is it possible to anchor knowledge about AI? The authors are of the view that it is helpful to consider the AI landscape in terms of the following four key questions.

- "What is AI?" It is important to know what the technology actually is, so as to understand what it can/cannot do and how its features may affect the way existing laws are applied (eg, tort, product liability). Also, if the use of AI (as opposed to AI itself) is to be regulated, AI must be clearly defined in order to determine whether or not a particular use is covered based on the underlying technology.
- "How should the use of AI be governed?" This is an exploration of the principles that govern the use of AI, with the aim of making the use of AI as safe as possible. Many countries around the world have set out their own frameworks. From Singapore's voluntary Model Framework to the Artificial Intelligence Act in the EU, there is an emerging global consensus on how the use of AI should be governed.
- "Is (the use of) AI what it is claimed to be?" For guidelines or legislation on AI governance to be effective, there must be a means to measure compliance with them, which is where testing and auditing come in. Singapore has developed self-assessment guides for organisations, as well as the aforementioned series of process and technical checks known as "AI Verify". By way of another example, the EU has introduced the concept of "conformity assessments", which evaluate how the AI system complies with the requirements in the EU's AI Act before the AI system is placed on the market.
- "What happens when things go wrong?" Every effort is made to ensure that the use of AI is as safe as possible. Nonetheless, there will still be cases where the use of AI results

in harm to a person or property, because risks can be reduced but not eliminated entirely – even though the governance principles certainly help with this. The harm could materialise as death, injury or property damage; however, there is also a risk of discrimination against a person. Therefore, there must be remedies available to ensure that the injured party is restored – whether via tort law, contract, etc.

Accordingly, recent trends and developments in Singapore will be discussed in this context.

Definition of AI and how this affects the way existing laws are applied

Many countries are aligning their definition of AI systems with the OECD's, which defines AI by its unique traits of autonomy and adaptiveness, and ASEAN (a political and economic union of ten South-East Asian nations, including Singapore) is no exception. The ASEAN Guide on AI Governance and Ethics defines an AI system as "a machine-based system that is capable of influencing the environment by producing an output (predictions, recommendations or decisions) for a given set of objectives", which "uses machine and/or human-based data and inputs to (i) perceive real and/or virtual environments; (ii) abstract these perceptions into models through analysis in an automated manner (eg, with machine learning), or manually; and (iii) use model inference to formulate options for outcomes" – further noting that "AI systems are designed to operate with varying levels of autonomy".

What the authors would like to share is based on their understanding of AI and how training is undertaken. In their view, three unique features require a closer look at how existing laws (especially those concerning fault-based liability) might apply to AI, as follows.

- AI is a "black box" – this affects how its workings are explained, as it is not always possible to explain how or why the AI system reached a particular outcome and the type of model chosen affects how easily its workings can be explained.
- AI is self-learning/autonomous – it is able to learn from the data it has been exposed to during its training and improve without being explicitly programmed, so the behaviour of the AI system is not always foreseeable.
- AI has many people involved in its development – from procuring the datasets, training and selecting the algorithm, to monitoring the performance of the algorithm. So who should be held responsible if the AI causes harm or its output is not as expected?

How the use of AI should be governed

In relation to traditional AI systems, this is covered by the second edition of the above-mentioned Model Framework issued by the IMDA/PDPC in January 2020 (the first edition was issued in January 2019). This Model Framework is sector-agnostic, meaning regulators can also issue guidance relevant to their sector as needed.

What are the key features of the Model Framework?

The Model Framework sets out ethics and governance principles for the use of AI, alongside practical recommendations that organisations can adopt to fulfil these principles. It is based on two high-level guiding principles that aim to promote public trust in and understanding of the use of AI, as follows.

- First, organisations using AI in decision-making must ensure that the decision-making process is:

(a) explainable – ensuring that the reasons behind the decision can be explained in non-technical terms;
(b) transparent – informing people that AI is being used in respect of them and how it affects them; and
(c) fair – ensuring that decisions do not create discriminatory or unjust impacts across different demographic lines (eg, race or sex).

- Second, AI solutions must be "human-centric" – meaning that the protection of human interests (including well-being and safety) should be the primary considerations when designing, developing and deploying AI.

The Model Framework also sets out the following four key areas in which organisations should follow its recommendations so as to promote the responsible use of AI:

- adapting or setting up internal governance structures and measures to incorporate values, minimise risks and allocate responsibilities relating to the use of AI;
- determining the appropriate level of human involvement in AI-augmented decision-making;
- operations management (ranging from selecting the datasets to choosing the algorithm) whereby the organisation must be alert to potential issues when developing, selecting and maintaining AI models; and
- interacting and communicating with the organisation's stakeholders who are affected by the use of AI.

It is recommended that these measures are explored throughout the development and deployment of AI – the life cycle of which can be summarised as follows.

- Stage 1 (gathering input) – selecting data that is to be input into the model for training purposes and, subsequently, when the model is deployed. As the accuracy of an AI model's output depends on the data that it is trained on, it is important to ensure that the data used is neither inaccurate (ie, drawn from incomplete records or outdated) nor biased (ie, not drawn from a representative group). Personal data must be processed in compliance with the Personal Data Protection Act 2012.
- Stage 2 (setting the decision-making process) – choosing the model, training the model, and calibrating the model based on the results of the training. The organisation must consult persons with expertise in order to identify suitable algorithms to analyse the data, and thereafter train the model and evaluate its performance until it produces a satisfactory level of accuracy.
- Stage 3 (output) – being able to explain why and how the model produced any output (eg, what factors it takes into account), so as to build trust in the use of AI and ensure that a person has sufficient information to frame their appeal if they wish to challenge the decision. If explainability is not possible, given the state of technology, the repeatability of the results should be demonstrated instead (where the same scenario will consistently give rise to the same outcome).
- Stage 4 (human review) – whether it is necessary for a human to review the decision made by the AI system before the decision is implemented will depend on a number of factors, including:
  (a) the severity of the harm to the individual – for example, compare the impact of a medical diagnosis with that of an online shopping recommendation;
  (b) the probability of the harm materialising;

(c) the nature of the harm (eg, physical or intangible);
(d) the reversibility of the harm and the availability of recourse; and
(e) whether it is operationally feasible to involve a human in the decision-making process – for example, in the case of a ride-hailing transportation service, there would be thousands of trip allocations per minute.

As regards general governance principles, the organisation must ensure it has robust oversight over its use of AI. This means that all persons involved in AI development and deployment should have clear roles and responsibilities, adequate training and resources, and the organisation's top management/board of directors must also play an active role in setting AI governance policies.

Organisations also need to keep records of the AI development process, starting with a data provenance record to track the origin/source of the (training) data and any changes made to it. The model training and selection process should be documented – along with the reasons why certain decisions were made and measures taken to address any risks identified. These records might be used in the future to troubleshoot where the AI system does not perform as expected or to defend against liability.

Finally, strong personal data protection and cybersecurity practices are required to be in place when using AI. However, given that such requirements are not unique to the use of AI, they are not discussed in this article.

In relation to generative AI systems, as previously mentioned, the Model Gen-AI Framework sets out the following nine areas to focus on in order to achieve trustworthy generative AI, along with the recommended actions to take for both industry and regulators.

- Accountability – responsibility should be allocated across the multiple players in the AI development chain (eg, model developers, deployers, and cloud service providers who host AI applications), based on the level of control each player has in the chain (drawing parallels with the cloud industry).
- Data – the quality of the data used in model training will affect the quality of its output; hence, while there is a need to increase data accessibility, there is also a corresponding need to ensure data (including personal data and data subject to copyright) is used lawfully.
- Trusted model development and application deployment – the industry must adopt best practices such as Retrieval-Augmented Generation to reduce hallucinations and have a standardised way to evaluate the performance and safety of generative AI models.
- Incident reporting – AI developers must report (and then patch) safety vulnerabilities in their AI systems and deployers must report serious incidents arising from their use of the AI system.
- Testing and assurance – both regulators and international standard-setting organisations should develop common standards for AI testing to be carried out by independent third parties.
- Security – tools must be developed to address the threats specific to generative AI.
- Content provenance – consumers should be aware they are interacting with AI-generated content and this calls for solutions such as watermarking, cryptographic provenance and public education.

- Safety and alignment R&D – this should be done to improve model safety, with global co-operation.
- AI for the public good – AI should improve people's lives and be environmentally sustainable.

Does Singapore take a different approach to the regulation of AI use?

There are two issues to consider when comparing Singapore's approach towards regulating the use of AI with approaches taken by other jurisdictions. The first looks at what kind of AI governance principles should apply and the second concerns how to implement those principles (ie, whether by means of legislation or guidelines only).

Singapore broadly resembles countries around the world in terms of the principles it believes should apply to the use of AI. A survey by the authors reveals there is growing international consensus between the EU, the USA, Japan, Australia, China and the UK in respect of the following principles.

- High-risk uses of AI should be subject to more requirements/safeguards than low-risk uses, where the concept of "risk" refers to the severity of the impact of the use of AI on the human.
- Decisions made by AI should be explainable, so that people know how and why the AI system makes a decision.
- The use of AI to make decisions should be fair and aim to minimise bias.
- The use of AI should be disclosed to persons affected by it (transparency).
- There must be means of applying for an appeal or review of the decision where it has a significant impact on the person.

However, when it comes to implementing these principles, approaches vary. The EU and Canada have introduced legislation – the EU AI Act and the Artificial Intelligence and Data Act, respectively – that regulates high-risk uses of AI and imposes certain obligations (generally) on the developers of such AI systems. However, Singapore, the UK, Japan and Australia have yet to take legislative steps and instead have issued guidelines and notices – while monitoring the industry to see if further action is necessary.

Each approach has its own strengths. Ultimately, it is up to each country to find the right balance between encouraging innovation and ensuring safety in the use of AI. However, the one consistent thing that countries are moving towards is interoperability in their AI governance, so as to remain attractive to foreign companies wishing to operate in their jurisdiction and also so that local companies can easily export their AI technology.

How compliance with AI governance principles is measured

Testing is a very important component of AI governance, as it enables various parties – including regulators, the organisation deploying the AI system, and the persons who are subject to decisions made by the AI system – to find out whether or not the AI system does indeed conform to the governance principles. In other words, it lets people see if the expectation matches up to the reality.

Testing matters because, if the use of AI is to be regulated through legislation (with sanctions for non-compliance), there needs to be a reliable and objective method to ascertain that it does indeed live up to the standards. Testing can be by way of self-assessment, or conducted by a third party, and it can be done by a series of

process checks – for example, reviewing documentation – or technical tools (or a combination of both).

In Singapore, the Model Framework is to be read in tandem with the Implementation and Self-Assessment Guide for Organisations (ISAGO), which sets out a series of questions for organisations to review in order to self-assess their compliance with the principles contained within the Model Framework.

May 2022 saw the launch of AI Verify, which consists of technical tests and process checks that let AI developers validate their claims about their AI systems against a set of 11 internationally accepted principles. The test results are not pass/fail, and do not guarantee that the AI system is free from bias or is completely safe, but confer the following positives:

- the results can be used to identify potential areas for improvement, as they come with recommendations for organisations; and
- the results are an objective and verifiable way for an organisation to demonstrate that it has implemented AI responsibly and ethically.

Liability when AI does not perform as expected

The use of AI carries two types of risks – namely, safety risks (eg, death, bodily injury, or property damage) and "fundamental rights risks" (to borrow the EU's description of rights risks such as discrimination, manipulation, or loss of privacy). The type of risk presented depends on how the AI system is used – for example, whether it is controlling an AV or screening CVs for recruitment.

Whether in the form of guidelines or legislation, the AI governance principles are there to ensure that the use of AI is as safe as possible and thereby minimise the likelihood of a risk occurring. An organisation can reduce the likelihood of a decision with discriminatory effects occurring by, for example, ensuring that the datasets used to train its AI model are representative of the population for which it is intended. The output produced by the AI system will be more accurate a result and therefore less likely to have an incorrect outcome and cause loss or damage.

However, despite every effort to ensure that the datasets are representative and testing is sufficient, there will still be adverse outcomes sometimes. It is worth bearing in mind that the same risks come with decisions or actions carried out by humans, who of course have their own unconscious bias. Hence, when the harm sought to be prevented arises, the focus must switch to compensating – or restoring – the affected party.

There is no quick or easy solution to this issue. In September 2022, an EU AI Liability Directive introduced a presumption of causality and powers to order disclosure of evidence to aid plaintiffs in bringing claims. Meanwhile, on 29 March 2023, the UK stated that it would not be making any changes to its current liability rules without prior industry consultation.

Singapore has not yet announced plans to introduce any legislation on liability. However, the authors are confident that the Singapore courts will be able to apply existing legal principles to this AI technology. Parliament has expressed similar confidence when discussing liability for AV accidents in 2017:

"The traditional basis of claims for negligence may not work so well where there is no driver in control of a vehicle. When presented with novel technologies, courts often try to draw analo-

gies to legal constructs in other existing technologies. In the case of AVs, the courts have autopilot systems for airplanes and autopilot navigational systems for maritime vessels, and product liability law to draw references from. As with accidents involving human-driven vehicles, it is likely that issues of liability for AVs will be resolved through proof of fault, and existing common law."

Liability for AI-generated content

This is something that every country will have to grapple with, following the advent of generative AI. Singapore has not had a reported case yet – although the Chief Justice has mentioned that courts have had self-represented persons use ChatGPT to write their submissions, which contained non-existent case law (however, no sanctions were reported). To the extent a person publishes AI-generated content, they can be liable as though they had generated the content themselves if the content is false, defamatory or harmful/toxic (eg, content that is an offence to post publicly under Singapore's laws).

However, when stepping back to look at the developer/deployer of the generative AI system, whether liability arises for AI-generated content may depend on whether the person deploying the AI system had a duty to provide correct information to the recipient of information from the AI system (such as in a company-customer relationship – eg, an airline providing information to its customers on special airfare rates – or if there was a professional duty to provide correct information), as they cannot delegate that duty to a generative AI system and then blame the developer. It may also turn on whether the output that is wrong is so harmless or trivial that reliance on it would not affect the recipient's rights (eg, the right to claim compensation).

To the extent that the output is toxic (eg, identity attacks, sexually explicit content, or language that incites violence) – as set out in the IMDA's Generative AI: Implications for Trust and Governance paper of June 2023 – it is arguable that the developer of the generative AI system will not be liable for the output if the developer had:

- implemented technological methods commonly used in the industry to reduce such toxic output (eg, content filters);
- posted clear warnings to users that the content may be offensive or inaccurate and made it a condition of use that they do not circumvent any guardrails (eg, content filters) in place;
- a mechanism for users to report any toxic content generated; and
- taken prompt action on any reports of toxic content generated.

Conclusion

AI is definitely here to stay, as Singapore now sees it as a necessity – rather than something just "good to have" – and champions its responsible use. While countries decide what regulatory levers are most appropriate to shape its use (legislation or voluntary guidelines), they are all striving towards interoperability of their AI governance frameworks, given how easily the technology flows across geographical borders.

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 Katie.Burrington@chambers.com