
CHAMBERS GLOBAL PRACTICE GUIDES

Artificial Intelligence 2023

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

**Singapore: Law & Practice
and
Singapore: Trends & Developments**

Chong Kin Lim and Cheryl Seah
Drew & Napier



SINGAPORE



Law and Practice

Contributed by:

Chong Kin Lim and Cheryl Seah

Drew & Napier

Contents

1. General Legal Framework p.4

1.1 General Legal Background Framework p.4

2. Industry Use of AI and Machine Learning p.5

2.1 Industry Use p.5

3. Legislation and Directives p.5

3.1 Jurisdictional Law p.5

3.2 EU Law p.6

3.3 US State Law p.6

4. Judicial Decisions p.6

4.1 Judicial Decisions p.6

4.2 Technology Definitions p.7

5. AI Regulatory Regimes p.7

5.1 Key Regulatory Agencies p.7

5.2 Technology Definitions p.7

5.3 Regulatory Objectives p.8

5.4 Enforcement Actions p.8

6. Proposed Legislation and Regulations p.8

6.1 Proposed Legislation and Regulations p.8

7. Standard-Setting Bodies p.8

7.1 National Standard-Setting Bodies p.8

7.2 International Standard-Setting Bodies p.9

8. Government Use of AI p.9

8.1 Government Use of AI p.9

8.2 Judicial Decisions p.10

8.3 National Security p.10

9. Generative AI p.10

9.1 Generative AI p.10

10. AI in the Practice of Law p.11

10.1 Uses of AI in the Practice of Law p.11

10.2 Ethical Considerations p.12

11. Theories of Liability p.12

11.1 Theories of Liability p.12

11.2 Regulatory p.14

12. General Technology-Driven AI Legal Issues p.14

12.1 Algorithmic Bias p.14

12.2 Data Protection and Privacy p.15

12.3 Facial Recognition and Biometrics p.16

12.4 Automated Decision-Making p.16

12.5 Transparency p.17

12.6 Anti-competitive Conduct p.17

13. Sustainability and Climate Change p.18

13.1 Sustainability and Climate Change p.18

14. AI in Employment p.18

14.1 Hiring Practices and Termination of Employment Practices p.18

14.2 Employee Evaluation and Monitoring p.18

15. AI in Industry Sectors p.19

15.1 Digital Platform Companies p.19

15.2 Financial Services p.19

15.3 Healthcare p.20

16. Intellectual Property p.20

16.1 Applicability of Patent and Copyright Law p.20

16.2 Applicability of Trade Secret and Similar Protection p.20

16.3 AI-Generated Works of Art and Works of Authorship p.21

16.4 OpenAI p.21

17. Issues for In-House Attorneys p.21

17.1 AI Issues for In-House Attorneys p.21

18. Advising Corporate Boards of Directors p.21

18.1 Advising Directors p.21

Drew & Napier 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 ex-

tensive experience in infocommunications, 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 include global and regional telecommunications service providers, sectoral regulators (both local and foreign), consultants, software houses, hardware manufacturers and international law firms.

Authors



Chong Kin Lim is the managing director of Drew & Napier's corporate & finance department. He heads the firm's TMT practice and co-heads both its data protection, privacy and

cybersecurity practice and its competition law and regulatory practice. With his strong background in competition, data protection and technology laws, Chong Kin 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. Her key areas of practice are TMT and administrative and public law. Cheryl advises

clients on legal issues surrounding the use of AI – from compliance with Singapore's data protection laws when using AI to process personal data to the IP and liability issues arising from the implementation of a ChatGPT-like system in the workplace. Cheryl was previously a state counsel/legislative drafter in the legislation division of the Attorney General's Chambers (Singapore's national law drafting office), where she drafted legislation across a wide variety of subjects – with a focus 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 Framework

Singapore unveiled its 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.

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 **3.1 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 **15.3 Healthcare** for further details).

Singapore currently has a set of voluntary guidelines – the Model Artificial Intelligence Governance Framework (Second Edition) (the “Model Framework”) – in place, which were issued by the Infocomm Media Development Authority

(IMDA) and the Personal Data Protection Commission (PDPC) in 2020. The Model Framework states that the use of AI should be fair, explainable, transparent and human-centric. The Model Framework is complemented by the Implementation and Self-Assessment Guide for Organisations (ISAGO), which provides a set of questions and examples for organisations to use when self-assessing how their AI governance practices align with the Model Framework. “AI Verify”, a self-assessment framework comprising both technical tests and process checks, was also rolled out in May 2022.

Regulators also issue guidance notes for industries, including the following.

- 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 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 Ministry of Health, 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 AI-MDs.

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.

2. Industry 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. Pursuant to its National AI strategy, Singapore has embarked on an initial tranche of five national AI projects, focusing on:

- intelligent freight planning to optimise the movement of freight;
- seamless and efficient municipal services;
- chronic disease prediction and management;
- personalised education through adaptive learning and assessment; and
- border clearance operations.

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.

3. Legislation and Directives

3.1 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 Framework**, 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 – autonomous vehicles (AVs) and AI-MDs.

In keeping with many jurisdictions around the world, Singapore has amended its road traffic legislation to accommodate the use of AVs, as this was previously premised on there being a human driver. 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.

As regards AI-MDs, the HPA requires medical devices to be registered. AI-MDs are a type of “medical device” (as defined in the HPA) but are subject to further requirements for registration by the Health Sciences Authority (HSA)’s Regulatory Guidelines for Software Medical Devices (see **15.3 Healthcare** for further details).

3.2 EU Law

3.2.1 Jurisdictional Commonalities

The matter is not applicable in this jurisdiction.

3.2.2 Jurisdictional Conflicts

The matter is not applicable in this jurisdiction.

3.3 US State Law

The matter is not applicable in this jurisdiction.

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 Generative 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 Ethereum/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 due to human error.

The Court of Appeal 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 of Appeal 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)). 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.

However, the remarks of Jonathan Mance J (dissenting) (at (193)) are of great applicability moving forward: “The law must be adapted to the new world of algorithmic programmes and artificial intelligence, in a way which gives rise to the results that reason and justice would lead one to expect.”

5. AI Regulatory Regimes

5.1 Key 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 Strategy in 2019. A National AI Office was also established under the SNDGO in order to set the national agenda for AI, as well as partner the research community and industry to implement the National AI Strategy.
- 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 bal-

ance the protection of an individual’s personal data with organisations’ need to use it. The IMDA/PDPC issued the Model Framework, which is sector-agnostic.

- 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.

5.2 Technology Definitions

The Model Framework 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.

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 promote the use of AI in Singapore in a way that is in line with internationally accepted principles by, for example, ensuring that:

- the decision-making process is explainable, transparent and fair when AI is used to make decisions; and
- AI solutions are human-centric (ie, promote the well-being and safety of humans).

As per (2.7) of the Model Framework, this is to build public trust in the use of AI 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.

The regulatory scope of specific agencies is set out in **5.1 Key Regulatory Agencies**.

5.4 Enforcement Actions

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

6. Proposed Legislation and Regulations

6.1 Proposed Legislation and Regulations

There is no indication that legislation regulating the use of AI will be introduced in the near future. As mentioned in **3.1 Jurisdictional Law**, Singapore’s approach for now is to issue guidelines in

order to help industries understand and navigate this rapidly evolving field.

During a Parliament sitting on 4 March 2020, the Minister for Communications and Information was asked whether the government was considering formulating regulations that would be binding on locally deployed AI systems so as to ensure the ethical and safe use of AI. The Minister replied that, as AI technology is still nascent, the Ministry of Communications and Information (MCI) does not have immediate plans to introduce new laws to regulate AI. The Minister highlighted other initiatives to ensure the safe and ethical use of AI – for example, the Model Framework and MAS’ FEAT principles – and stated that the MCI and the PDPC would continue to monitor global developments.

7. Standard-Setting Bodies

7.1 National Standard-Setting Bodies

Enterprise Singapore oversees the setting of standards in Singapore. Through the industry-led Singapore Standards Council (SSC), it administers the Singapore Standardisation Programme, which develops and promotes standards in Singapore.

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.

7.2 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). Singapore is also a member of the UNCITRAL Working Group IV (Electronic Commerce) looking into the use of AI and automation in contracting.

AI Singapore (see 5.1 Key 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.

8. Government Use of AI

8.1 Government Use of AI

Across the Singapore government, AI solutions are being adopted in line with Singapore’s Smart Nation Initiative to leverage technology to make impactful changes to the nation and the economy. The following are among examples of such.

- 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.
- The Singapore Police Force (SPF) intends to increase its camera network to more than 200,000 cameras by 2030 in an effort to deter criminals and safeguard Singapore’s public housing estates. In order to cope with the already high volumes of footage, the SPF utilises AI to analyse footage and improve their response against crimes and security threats.
- The SPF also partnered with the National Crime Prevention Council and GovTech to develop the “ScamShield” application to combat scams. ScamShield uses AI technology to filter scam messages through the identification of keywords and blocks calls from blacklisted numbers.
- The Home Team Science and Technology Agency has trialled Xavier, an autonomous ground robot, to patrol public areas with high foot traffic in an effort to enhance public health and safety. Footage from Xavier’s cameras is streamed to a video analytics system with AI capability, which allows public officers to activate additional resources to respond to on-ground situations if necessary.

- The Singapore Food Agency, together with GovTech, developed an AI and image recognition technology to automate the counting of rotifers, a type of plankton critical to feeding marine fish larvae. This reduced the daily time taken for this process from 40 minutes to one minute.

In February 2023, the government announced that a pilot project known as “Pair” was being developed and trialled across a number of government agencies. Pair integrates ChatGPT into Microsoft Word to assist public officers in their writing and research. In order to ensure data security and confidentiality, the government has struck an agreement with Azure OpenAI, the Large Language Model provider, to keep confidential information from 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.

8.2 Judicial Decisions

However, the Singapore courts are unlikely to use AI tools – for example, 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.

8.3 National Security

The Ministry of Defence and the Singapore Armed Forces (SAF) have been exploring the use of AI in military operations to enhance capabili-

ties 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.

9. Generative AI

9.1 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

The extent to which one may use copyrighted content to train Generative AI models is not clear in Singapore and the rest of the world. There are no cases brought before the Singapore courts yet. We note that lawsuits have been filed in the USA against AI-powered coding assistants, which have been trained on public repositories of code on the internet, and reproduce open-source code without crediting the creators of the code. There are also ongoing lawsuits overseas against AI art generators, in which an image company alleges that millions of its images were used to train the AI model with neither permis-

sion nor compensation. The outcomes of these lawsuits will be relevant to Singapore.

In Singapore, under Section 244 of the Copyright Act 2021, use of copyrighted works is permitted where a copy of the work is made for the purpose of computational data analysis (as defined in Section 243 of the Copyright Act 2021) or preparing the work for computational data analysis, provided that certain conditions are met. Section 244 of the Copyright Act 2021 has 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. Much of the debate concerns whether AI is seen as a mere tool (akin to a paintbrush) when producing output or, where the machine determines how to implement the human's instructions, whether it is more akin to instructing a commissioned artist.

In relation to copyright, the current position under the Copyright Act 2021 is that the author must be a natural person. However, 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 depend-

ing 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. Large Language Models like 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 this defence has not yet been tested in 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.

The law is moving very fast in this area, with regulators overseas committing to issuing guidelines in the next few months. For more details on IP protection of an AI system itself (and not its output), please see **16.1 Applicability of Patent and Copyright Law** and **16.2 Applicability of Trade Secret and Similar Protection**.

10. AI in the Practice of Law

10.1 Uses of AI in the Practice of Law

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.

The Second Minister for Law, Edwin Tong, has said AI cannot replace lawyers when it comes to finding the best way to fulfil a client’s need. When speaking at the TechLaw.Fest (an annual conference on law and technology) in September 2022, the Second Minister said: “AI can help you with the base material, but it cannot replace the creativity that the lawyer can bring to the team.”

In October 2020, the Ministry of Law (“MinLaw”) launched the Legal Industry Technology and Innovation Roadmap (TIR), a ten-year plan that will help the legal industry harness technology to increase productivity. AI is seen as a means to reduce or eliminate rote tasks in order to free lawyers up for more valuable work that requires human attention. The TIR also suggested that AI could be used to carry out risk assessments and outcome simulations that would assist litigants on possible outcomes of a case and serve as guidelines for judges.

10.2 Ethical Considerations

Is a lawyer able to discharge their professional responsibilities if they do not understand how the technology works or they cannot explain why the AI system chose one course of action over another? This may depend on the level of safeguards put in place.

A lawyer does not necessarily need to understand precisely how the AI system works from a technical perspective; however, they must understand what the AI system is capable of doing, how it arrives at a result, what it was trained on (eg, whether the dataset is relevant), and what its limitations are. There is also the risk of automation bias, where humans defer to

the perceived superiority of the AI technology instead of choosing to override its decision.

Another issue to be considered is the level of accuracy of the AI system that is used. In a case where a lawyer is using ChatGPT to conduct research or summarise a case, the lawyer should check to ensure the output is correct, as ChatGPT is known to “hallucinate” (ie, produce made-up answers). However, if the AI tool has an accuracy of 98% when it comes to identifying relevant documents, it still means that 2% of documents slip through the cracks. The law firm must come up with a strategy to manage this risk.

11. Theories of Liability

11.1 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 Quoine case mentioned in **4.1 Judicial Decisions** involved human failure rather than a failure of the algorithms.) The Model Framework does not discuss liability either.

The authors are of the view that there are three features of AI that may affect the application of conventional principles of liability, namely:

- 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, meaning 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. While the European Parliament has recommended taking the position that the “operator” of the AI system – ie, the person who controls the risks associated with it – should be liable, there are no such formal proposals in Singapore yet.

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).

Despite the challenges posed by the nature of AI, the courts will take a measured and incremental approach to determining liability. In the context of AVs, 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.”

In any case, the victim will not be left without a remedy. The Road Traffic Act 1961 requires an insurance policy indemnifying the owner and any authorised driver or operator of the vehicle in relation to death or bodily injury or damage to property caused by – or arising from – the use of the vehicle. If there is no liability insurance, a security deposit of not less than SGD1.5 million must be placed with the LTA.

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 like 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 their 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.

11.2 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).

12. General Technology-Driven AI Legal Issues

12.1 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 Implementation and Self-Assessment Guide for Organisations will also help organisations to reduce bias in the AI development process.

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

12.2 Data Protection and Privacy

The collection, use and disclosure of personal data in Singapore is subject to the Personal Data Protection Act 2012 (PDPA).

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, with the exception of obtaining consent from the individual, some of the more 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 assessment; 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 – Uses and Risk of Re-Identification

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.

Organisations should therefore not take for granted that their data is anonymised and will always remain so. Once an organisation is using “personal data”, it must comply with the obligations under the PDPA.

Nevertheless, where data is anonymised, generally organisations must not be able to use that data as personal data – for example, the data cannot be used to make a decision about (or in a manner that has a targeted impact on) a specific individual. The organisation would otherwise in effect be using the data as personal data and must ensure that consent has been obtained for such use, unless any exceptions apply. See the Advisory Guidelines on the PDPA for Selected Topics at (3.41).

12.3 Facial Recognition and Biometrics

By 2025, as part of Singapore's National AI Strategy, facial recognition, iris and fingerprint identification will be implemented at all of Singapore's immigration checkpoints to provide automated immigration clearance.

The key legal issue around facial recognition and biometrics in Singapore is that of data protection. 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 liveness 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.

12.4 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 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.

12.5 Transparency

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). This will build trust in the use of AI.

Additionally, organisations are advised to explain to consumers how decisions made with the use of AI can affect them (eg, what factors will be taken into account) and how they can contest such decisions where necessary.

12.6 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 organisa-

tion 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.

13. Sustainability and Climate Change

13.1 Sustainability and Climate Change

The National Environment Agency (NEA) and Public Utilities Board (PUB) use AI technologies for environmental monitoring and natural resource management. As Singapore is affected by transboundary haze, the NEA's Meteorological Service Singapore used AI to process vast amounts of satellite data to develop a haze tracking system and multi-satellite fire-detection product. This allows for early detection of fires and haze in the region and helps agencies better plan their operations and deploy resources. The PUB has also implemented radar and machine learning algorithms to enhance the Radar Rainfall Monitoring System, which improves the forecasting of heavy rainfall locations and allows for the timely deployment of PUB's Quick Response Team to areas at risk of flash floods.

The Energy Market Authority (EMA) is also funding SGD6.2 million to develop Singapore's solar forecasting capabilities and a consortium is looking into improving the accuracy of solar energy output forecasts and grid management through weather prediction, remote sensing, machine learning and grid modelling.

14. AI in Employment

14.1 Hiring Practices and Termination of Employment 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.

14.2 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 circum-

stances — 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 through, for example, 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.

15. AI in Industry Sectors

15.1 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 Minister for Manpower declared that Ministry of Manpower (MOM) 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.

15.2 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 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 presently leads an industry consortium (“Veritas”) that creates frameworks for responsible use of AI. Phase 1 concluded on 6 January 2021 with the online publication of two White Papers, thereby setting out a methodology to assess fairness for credit-risk scoring and customer marketing.

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.

15.3 Healthcare

As mentioned in **1.1 General Legal Background Framework**, AI-MDs must be registered under the HPA before they are used. The HSA's Regulatory Guidelines for Software Medical Devices sets out additional information that 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.

16. Intellectual Property

16.1 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.
- 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 as 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, the actual contribution of the claimed subject matter is likely considered to go beyond the underlying mathematical method and thus could be regarded as an invention. 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 **9.1 Generative AI**.

16.2 Applicability of Trade Secret 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 to 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.

AI-Generated Works of Art and Works of Authorship

The protection of the output of Generative AI systems under copyright and/or patent laws is discussed in **9.1 Generative AI**.

16.3 AI-Generated Works of Art and Works of Authorship

See the issues outlined in **9.1 Generative AI**.

16.4 OpenAI

See the issues outlined in **9.1 Generative AI**.

17. Issues for In-House Attorneys

17.1 AI Issues for In-House Attorneys

In-house attorneys should keep abreast of developments in the AI sphere, as the technology knows no borders. Legislation and guidelines enacted in other countries could have an impact on their company, especially if their company exports its AI technology or performs services using its own AI technology for overseas companies.

Additionally, in-house attorneys should have an understanding of the AI technology involved – for example, how a Large Language Model functions. This will enable them to effectively advise on matters arising from the use of AI in the company's operations.

18. Advising Corporate Boards of Directors

18.1 Advising Directors

When deploying AI solutions, a company's board of directors 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 coordinating 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 should be guided by the organisation's corporate values. The board of directors need to strike a balance between the commercial objectives/advantages of using AI and the risks of using AI. For more details, please see **12.4 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. The departments responsible for the quality of data, model training and model selection should work together to understand the lineage of the data used, ensure data quality, minimise any inherent bias in the datasets, and periodically review and update 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 board of directors should consider how to build consumers' trust in their organisation's 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 and queries or apply for a review of a decision made by the AI system.

Trends and Developments

Contributed by:

Chong Kin Lim and Cheryl Seah

Drew & Napier

Drew & Napier 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 ex-

tensive experience in infocommunications, 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 include global and regional telecommunications service providers, sectoral regulators (both local and foreign), consultants, software houses, hardware manufacturers and international law firms.

Authors



Chong Kin Lim is the managing director of Drew & Napier's corporate & finance department. He heads the firm's TMT practice and co-heads both its data protection, privacy and

cybersecurity practice and its competition law and regulatory practice. With his strong background in competition, data protection and technology laws, Chong Kin 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. Her key areas of practice are TMT and administrative and public law. Cheryl advises

clients on legal issues surrounding the use of AI – from compliance with Singapore's data protection laws when using AI to process personal data to IP and liability issues arising from the implementation of a ChatGPT-like system in the workplace. Cheryl was previously a state counsel/legislative drafter in the legislation division of the Attorney General's Chambers (Singapore's national law drafting office), where she drafted legislation across a wide variety of subjects – with a focus 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's National AI Strategy was announced in 2019, revealing the country's aim to become a leader in developing and deploying scalable and impactful AI solutions by 2030 – along with its present focus on deploying AI in five key sectors (namely transport and logistics, municipal services, chronic disease prediction and management, education, and border safety and security). AI is also deployed beyond the above-mentioned five areas, however, across every industry from finance to food service. Indeed, robot waiters have been known to bring orders to tables in restaurants.

Singapore continues to enthusiastically embrace this technology. As recently as February 2023, it was announced that civil servants will soon be using a system built on ChatGPT to conduct research – as well as draft emails, reports and speeches – to improve their productivity.

Funding-wise, in November 2021, the government allocated an additional SGD180 million to AI research in the financial sector and in the delivery of public sector services (such as job-matching on the national jobs portal) – on top

of the SGD500 million previously committed to AI research activities. In October 2022, the government announced a further SGD71 million to develop the workforce's expertise in AI and opened three new centres of innovation for SMEs to test their new AI projects.

Additionally, a number of government policies complement the funding for research. The Intellectual Property Office of Singapore has implemented "SG IP FAST", which enables the acceleration of patent, trade mark and registered design applications in all technology sectors. Patent applications can now be granted in as quickly as six months, rather than taking two years or more.

There has also been a concerted effort to educate the public regarding AI, with a free online course ("AI for Everyone") conducted by AI Singapore (a multi-party effort between various economic agencies in Singapore and academia). The course explains the technology and also aims to dispel concerns such as "Will AI take over my job?".

When it comes to regulating the use of AI, Singapore takes a measured approach. 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 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 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);
- the IP and Artificial Intelligence Information Note issued by the Intellectual Property Office of Singapore to provide AI innovators with an overview of how to protect their AI inventions; 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/PDPC is 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 a 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 Artificial Intelligence 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

There are many definitions of AI – from the OECD’s to local definitions within each country. However, it is worth setting out the definition used in Singapore’s Model Framework, as it applies across all sectors. AI refers to “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)”.

There are also many websites, books and videos available that address what AI is, what machine learning is, and how a model is trained, etc. As a result, this article refrains from elaboration.

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.

- 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 is held responsible if the AI causes harm or its output is not as expected?

In a pro-innovation approach to AI regulation published on 29 March 2023, the UK recently took the step of using such unique characteristics to define AI as products and services that are “adaptable” (because AI systems, once trained, can find new patterns and connections in data

that are not directly envisioned by the human programmer) and “autonomous” (because AI systems can make decisions without the express intent or ongoing control of a human). This enables the UK to future-proof the definition (as opposed to listing specific technologies or applications of AI). Could this approach be the way forward in Singapore?

How the use of AI should be governed

The most well-known AI governance framework in Singapore is the second edition of the aforementioned Model Framework issued by the IMDA/PDPC in January 2020 (the first edition was released in January 2019). This Model Framework is sector-agnostic, meaning regulators can also issue guidance relevant to their sector as needed – for example, the MAS’ FEAT principles for the financial industry and the MOH/HSA’s specific guidelines for AI-enabled medical devices.

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.

- 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 persons 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 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) where 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 lifecycle 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.

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 USA and the EU have introduced legislation – the Algorithmic Accountability Act 2022 and the Artificial Intelligence 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.

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 eight internationally accepted principles.

Liability when AI does not perform as expected

The use of AI carries two types of risks – namely, safety risks (eg, death, bodily injury, property damage) and “fundamental rights risks” (to bor-

row 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 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 nor 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 analogies 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.”

Conclusion

At the end of the day, AI is here to stay. As such, Singapore should make the most of this technology. Laws (if any) could be led by existing technology or future-proofed to stay one step ahead. Either way, it is up to humans to ensure that the use of AI is shaped in a responsible and sustainable manner.

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