PANORAMIC NEXT

Artificial Intelligence

SINGAPORE

LEXOLOGY

Artificial Intelligence

2024

Contributing Editor

Theo Ling

Baker McKenzie

In this guide, a global panel of legal experts analyse the key trends and developments in the fast-evolving world of artificial intelligence. Through a series of engaging interviews, they discuss the most important legislative, regulatory and policy initiatives affecting AI developers and look at what the future may hold in this exciting field.

Generated: November 20, 2024

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. Copyright 2006 - 2024 Law Business Research

LEXOLOGY

Explore on **Lexology**

Singapore

Lim Chong Kin, **David N Alfred**, **Anastasia Su-Anne Chen**, **Cheryl Seah**
Drew & Napier LLC

Summary

PROFILES

About

Q&A

What is the current state of the law and regulation governing AI in your jurisdiction? How would you compare the level of regulation with that in other jurisdictions?

Has the government released a national strategy on AI? Are there any national efforts to create data sharing arrangements?

What is the government policy and strategy for managing the ethical and human rights issues raised by the deployment of AI?

What is the government policy and strategy for managing the national security and trade implications of AI? Are there any trade restrictions that may apply to AI-based products?

How are AI-related data protection and privacy issues being addressed? How will these issues affect data flows and data sharing arrangements?

How are government authorities enforcing and monitoring compliance with AI legislation, regulations and practice guidance? Which entities are issuing and enforcing regulations, strategies and frameworks with respect to AI?

Has your jurisdiction participated in any international frameworks for AI?

What have been the most noteworthy AI-related developments over the past year in your jurisdiction?

Which industry sectors have seen the most development in AI-based products and services in your jurisdiction? Are there any emerging industry or non-governmental standards governing the development and use of AI-related technologies?

Are there any pending or proposed legislative or regulatory initiatives in relation to AI?

What best practices would you recommend to assess and manage risks arising in the deployment of AI-related technologies, including those developed by third parties?

THE INSIDE TRACK

What skills and experiences have helped you to navigate AI issues as a lawyer?

Which areas of AI development are you most excited about and which do you think will offer the greatest opportunities?

What do you see as the greatest challenges facing both developers and society as a whole in relation to the deployment of AI?

Profiles

ABOUT

Lim Chong Kin is the managing director of Drew & Napier LLC's corporate and finance department. He heads the telecommunications, media & technology (TMT) practice, and co-heads the data protection, privacy & cybersecurity practice and competition law & regulatory practice.

Chong Kin played a key role in the liberalisation of the telecommunications, media and postal industries in Singapore. Since 1999, he routinely advises the sectoral regulators on liberalisation, market access, licensing, competition regulation, merger reviews and enforcement issues, including successfully defending the regulators in many Ministerial appeals. He was an early pioneer in the practice of competition laws in Singapore, through drafting of the competition frameworks that continue to govern the telecoms, media and postal sectors today. Chong Kin is also a pioneer in the practice of data protection, being relied upon by Singapore's data protection commission to draft their implementation guidelines, assist in complex enforcement of data breach cases, and develop cross-border frameworks. Besides Singapore, Chong Kin also acts for various ASEAN regulators on matters related to his expertise in competition, data and TMT.

Given Chong Kin's broad, deep and overlapping experience in competition, data and regulatory work, he is truly unique in being able to advise on complex matters spanning across the entire spectrum of the digital economy. Drawing on this unique background, Chong Kin frequently advises clients in the cutting-edge industries of AI, fintech, Big Data and TMT. He is equally adept at advising clients on market entry, telecommunications infrastructure deployment and data centre issues (hardcore TMT), to advising on all aspects of the data handling (focusing on data protection and cybersecurity), and into the new areas of AI and other 'killer applications' that are driving the digital economy.

As a testament to his standing, Chong Kin has consistently been recommended as a leading individual by all the major international legal publications across the areas of competition, data and TMT including *The Asia Pacific Legal 500*, *Global Competition Review*, *Chambers Asia-Pacific*, *The Guide to the World's Leading Competition & Antitrust Lawyers/Economists*, *Who's Who Legal*, *Practical Law Company Which Lawyer?*, *Asialaw Profiles* and *Best Lawyers*. He is also highly regarded by his peers, clients and rivals alike for his expertise. All the practices in competition, data and TMT that Chong Kin founded and continues to head in the firm, have been widely acclaimed as leading practices in Singapore.

Chong Kin is a senior accredited specialist in data and digital economy law by the Singapore Academy of Law.

David N Alfred is director and co-head of data protection, privacy and cybersecurity at Drew & Napier and a member of the firm's Artificial Intelligence (AI) and Digital Trust practice. He is also Co-Head and Programme Director of the Drew Data Protection & Cybersecurity Academy.

David is a senior technology lawyer with over 25 years' experience encompassing legal, public policy, business and technological aspects of the digital economy, data, digital

technology, telecommunications and the internet. He has particular expertise in data law and policy, digital and cyber regulation, data protection and cybersecurity.

David has spoken widely on global aspects of data governance, privacy and cybersecurity, development of data protection law in Southeast Asia, data protection management and compliance, AI regulation, digital trust and other technology and business-related topics. He has taught courses up to postgraduate level at local tertiary institutions and is a qualified corporate trainer and adult educator.

Prior to joining the firm, David was the first chief counsel to Singapore's Personal Data Protection Commission (from 2013 to 2020). He has also worked with Singapore's Info-communications Media Development Authority and its predecessor, the Info-communications Development Authority of Singapore.

David has been recognised as a senior accredited specialist in data and digital economy law by the Singapore Academy of Law and as a Fellow of Information Privacy by the IAPP.

Anastasia Su-Anne Chen is a director with the corporate &and finance department in Drew & Napier.

Her key areas of practice are technology, media, and telecommunications (TMT), data protection, privacy and cybersecurity, as well as artificial intelligence (AI) and digital trust.

Prior to joining the firm, Anastasia was Deputy Chief Counsel to Singapore's Personal Data Protection Commission (PDPC) and Info-communications Media Development Authority (IMDA) for over nine years. She was lead counsel for PDPC's matters, IMDA's procurement and intellectual property portfolios, as well as IMDA's Data Administration Group.

Anastasia has advised on a broad range of regulatory, compliance and commercial matters, both in her role as in-house counsel as well as in private practice. Her extensive experience includes advising on data protection compliance and management programmes, cross-border data transfers, data incident management and response, investigations and enforcement by the PDPC, AI governance clauses for vendor contracts, and legal risks arising from the development and deployment of large language models.

She has been recognised as a senior accredited specialist in data & digital economy law by the Singapore Academy of Law.

Cheryl Seah is a director with the corporate and finance department in Drew & Napier.

Her key areas of practice are telecommunications, media & technology (TMT), artificial intelligence (AI) and digital trust, as well as administrative and public law.

Cheryl advises clients on regulatory matters, ranging from cybersecurity to payment services to gaming. She also advises companies ranging from Fortune 500 MNCs to local and foreign start-ups on legal and governance issues arising from their use of AI 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.

Cheryl publishes frequently on legal issues arising from the use of AI with the Law Society of Singapore and has conducted talks on AI for external organisations (eg, IPOS International, LexisNexis SEA), local and ASEAN regulators, and local and European universities.

Before joining the firm in 2022, Cheryl was a state counsel/legislative drafter in the Legislation Division of the Attorney-General's Chambers (Singapore's national law drafting office). She has advised on and drafted legislation across a wide variety of subjects, with a focus on transport (including autonomous vehicles), infrastructure, technology and civil procedure.

Q&A

WHAT IS THE CURRENT STATE OF THE LAW AND REGULATION GOVERNING AI IN YOUR JURISDICTION? HOW WOULD YOU COMPARE THE LEVEL OF REGULATION WITH THAT IN OTHER JURISDICTIONS?

The use of AI in Singapore is regulated by a network of legislation, voluntary guidelines and case law.

In relation to legislation, existing laws such as laws relating to data protection, intellectual property, consumer protection and cybersecurity will apply to the use of AI. To the extent that AI is used to provide a service (eg, to assist in the provision of legal services), or is integrated into a product (eg, developing an AI-enabled medical device), the existing laws governing that product or service will apply.

While Singapore does not have an omnibus AI Act unlike the EU's that applies across multiple sectors, Singapore has enacted legislation in relation to specific applications of AI where necessary. For example, Singapore has legislation for autonomous vehicles (as existing road traffic laws were premised on there being a human in the driver's seat controlling the vehicle), and most recently (on 9 September 2924), the Elections (Integrity of Online Advertising) (Amendment) Bill was introduced in Parliament, tackling the issue of manipulated online content (deepfakes) in elections. Generative AI was listed as an example of digital means by which content could be generated or manipulated.

In relation to guidelines, the most significant ones that apply across all sectors are the Model AI Governance Framework (introduced in January 2019 and revised in January 2020), issued jointly by the Infocomm Media Development Authority (IMDA) and the Personal Data Protection Commission (PDPC) and the Model Governance Framework for Generative AI introduced in May 2024 by the IMDA and the AI Verify Foundation. These Model Governance Frameworks set out ethical principles governing the use of AI and practical steps organisations can take to give effect to these principles.

There are also sector-agnostic guidelines to help organisations in the development of AI systems, that relate to more specific aspects of AI systems, such as the use of personal data, and maintaining cybersecurity:

- PDPC – Advisory Guidelines on the use of Personal Data in AI Recommendation and Decision Systems (March 2024); and
- Cybersecurity Agency of Singapore – Guidelines on Securing AI Systems and the Companion Guide on Securing AI Systems (draft for public consultation in July 2024).

Lastly, there are also guidelines issued by sectorial regulators, such as:

-

the Monetary Authority of Singapore (MAS) has introduced the Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector (2018), together with a series of white papers to implement the FEAT principles in partnership with the industry; and

- the Artificial Intelligence in Healthcare Guidelines (2021), co-developed by the Ministry of Health and the Health Sciences Authority.

Where an AI system causes harm, principles of tort law and contract law will also apply to give the affected person a remedy. At present, we do not have judicial decisions on the application of artificial intelligence, although our Court of Appeal has decided on a case where algorithms were used in financial trading without the involvement of humans (*Quoine v B2C2* [2020] SGCA(I) 02).

In summary, Singapore's approach to the use of AI can be described as flexible and pragmatic. The government will leverage on guidelines as well as amendments to laws to ensure that AI is used responsibly while also supporting innovation. The government also ensures that its AI governance frameworks are in line with the international community's, such as in the adoption of AI ethics principles, and how to tackle the challenges and risks of AI use.

HAS THE GOVERNMENT RELEASED A NATIONAL STRATEGY ON AI? ARE THERE ANY NATIONAL EFFORTS TO CREATE DATA SHARING ARRANGEMENTS?

Singapore released its national strategy on AI in 2019 and has updated it in 2023.

The first national strategy focussed on an initial tranche of five national AI projects to deliver strong social and economic impact domestically, in the following areas: (1) freight planning; (2) improved delivery of municipal services; (3) chronic disease prediction and management; (4) personalised education experiences for each student through adaptive learning and assessment and (5) border clearance operations.

The updated 2023 national strategy makes three key shifts, where: (1) AI is now viewed as a 'necessity', rather than just a 'good to have'; (2) Singapore will expand from a local to global approach, connecting to global innovation networks to overcome the challenges surrounding AI (eg, energy, data and ethics), as well as contribute its expertise and product innovations; and (3) Singapore will move beyond the flagship national AI projects to administer AI-enabled solutions in all sectors of our economy and society.

In terms of national efforts to create data sharing arrangements, IMDA released a Trusted Data Sharing Framework in June 2019 to provide guidance to the industry, outlining key issues organisations should take into account when entering into partnerships to share both personal and business data. The Framework set out potential data sharing models, outlines legal and regulatory compliance requirements for data sharing, as well as the technical and organisational considerations, and also provides recommendations on ensuring transparency and accountability, and retaining and disposing of data, after the data has been shared.

As part of IMDA's guidance to organisations, it has also posted sample agreements (eg, agreements for bilateral data sharing or multilateral data sharing) on its website

, which organisations can adapt for their use as necessary in relation to the sharing of non-personal data.

WHAT IS THE GOVERNMENT POLICY AND STRATEGY FOR MANAGING THE ETHICAL AND HUMAN RIGHTS ISSUES RAISED BY THE DEPLOYMENT OF AI?

The government's strategy is twofold, where it utilises both laws and guidance to organisations. The guidelines set out recommended steps for organisations to take when they deploy AI systems to minimise the risk of discrimination, and the laws will target the discriminatory outcomes (independent of whether AI is used).

In terms of guidelines, the Model AI Framework and the Model Generative AI Framework set out recommendations to manage these ethical issues, such as:

- AI developers should adopt industry best practices in data governance – such as ensuring that the data used in training the model is representative and current, and where training datasets are labelled or annotated it is done consistently and accurately;
- the Model AI Framework sets out examples of how datasets can be biased (eg, selection bias and measurement bias) so that organisations are aware of it and can develop strategies to minimise such instances;
- if there is a coordinating body within the organisation for AI projects, it should have the relevant expertise and comprise diverse representatives from across the organisation; and
- to take on board feedback from stakeholders who will be impacted by the deployment of AI.

However, to give the guidelines 'teeth', the government also relies on laws. For example, in the employment context, if an employer is found to have discriminated against an individual on the basis of age, religion, race, gender or marital status, the government is able to take action against the employer regardless of whether the employer had used AI in making that decision. For example, the government may curtail the employer's work pass privileges, affecting their ability to hire employees. Workplace fairness legislation is targeted to be introduced later this year to prohibit workplace discrimination based on protected characteristics, and for employers to set up grievance handling processes for their employees.

WHAT IS THE GOVERNMENT POLICY AND STRATEGY FOR MANAGING THE NATIONAL SECURITY AND TRADE IMPLICATIONS OF AI? ARE THERE ANY TRADE RESTRICTIONS THAT MAY APPLY TO AI-BASED PRODUCTS?

The government acknowledges the increased risk of cyber-attacks as Singapore continues to digitalise. The Cybersecurity Act 2018 (CA) sets out the legal framework for the maintenance of national cybersecurity in Singapore. Regardless of whether an organisation uses AI in their operations, the following classes of organisations will be subject to the CA such that they must comply with varying levels of standards and directions, and discharge their reporting obligations to the authorities:

1. providers of essential services who own the critical information infrastructure used for the continuous delivery of the essential services they are responsible for;
2. providers of essential services who use third-party owned critical information infrastructure;
3. owners of systems of temporary cybersecurity concern (where these systems face higher risks of cyber-attacks – eg, pandemic vaccine distribution systems);
4. entities of special cybersecurity interest – eg, autonomous universities; and
5. providers of major foundational digital infrastructure services (eg, cloud computing service providers; data centre facility service providers).

In relation to the classes of persons mentioned in items (2) to (5), the legislative provisions are not yet in force at the time of writing.

The trade restrictions that apply to products (whether or not they are AI-based) can be found in legislation such as the Strategic Goods (Control) Act 2002 (which controls the transfer and brokering of goods and technology capable of being used to develop, produce, operate, stockpile or acquire weapons capable of causing mass destruction, among other purposes), as well as the Regulation of Imports and Exports Act 1995 (which, among other prohibitions, also sets out prohibitions on imports from and exports of certain goods to specified countries).

HOW ARE AI-RELATED DATA PROTECTION AND PRIVACY ISSUES BEING ADDRESSED? HOW WILL THESE ISSUES AFFECT DATA FLOWS AND DATA SHARING ARRANGEMENTS?

The Personal Data Protection Act 2012 (PDPA) governs the collection, use, disclosure and processing of personal data in the private sector and a separate, similar regime applies in relation to public sector entities under the Public Sector (Governance) Act 2018. In March 2024, following a public consultation in July 2023, the PDPC issued the Advisory Guidelines on the use of Personal Data in AI Recommendation and Decision Systems to clarify how the PDPA applies when organisations use personal data to develop and train AI systems.

The Advisory Guidelines cover what organisations must do at various stages of AI system implementation – namely (1) development, testing and monitoring, (2) deployment and (3) procuring a bespoke AI system trained on personal data the organisation holds – and set out the relevant legal bases for collection, use and disclosure of personal data at each stage. In general, all obligations under the PDPA will apply in relation to personal data that is collected, used and disclosed in connection with the development, training and deployment of AI systems.

In relation to collection, use and/or disclosure (sharing) of personal data of individuals for the purpose of training an AI model, an organisation may do so with the individuals' consent or if otherwise permitted to do so (without the individuals' consent) under the PDPA or any other written law. This may include, for example, in relation to certain business improvement purposes, for research and for an organisation's legitimate interests (subject to the conditions and requirements of the PDPA). If an organisation will be collecting, using or disclosing (sharing) personal data for purposes that are different from the original purposes they had collected the personal data for, the organisation must do so in accordance with the PDPA (ie, seek fresh consent unless such collection, use and/or

disclosure without consent is permitted under the PDPA), or seek an exemption from the PDPC.

Therefore, when entering into contractual arrangements governing data flows or data sharing, organisations will have to abide by the PDPA (and any other applicable law). While organisations cannot 'contract out' of the requirements of the PDPA, their contractual arrangements should define the parties' respective scope of responsibilities in relation to the protection of individuals' personal data and privacy.

HOW ARE GOVERNMENT AUTHORITIES ENFORCING AND MONITORING COMPLIANCE WITH AI LEGISLATION, REGULATIONS AND PRACTICE GUIDANCE? WHICH ENTITIES ARE ISSUING AND ENFORCING REGULATIONS, STRATEGIES AND FRAMEWORKS WITH RESPECT TO AI?

The use of AI in particular goods or services will be monitored by the relevant sectorial regulator. It does not come under the purview of a single or central regulator such as the IMDA, even though the IMDA and the PDPC have issued the Model Governance Frameworks that are of general application across sectors.

For example, where AI is used in financial services, such as robo-advisors, the MAS has issued Guidelines on the Provision of Digital Advisory Services, where organisations must minimally disclose in writing the following to their clients: (1) the assumptions, limitations and risks of the algorithms; (2) the circumstances under which the organisation may override the algorithms or temporarily halt the digital advisory service; and (3) any material adjustments to the algorithms.

In relation to the collection, use and disclosure of personal data to develop AI systems, or be processed by AI systems, the PDPC will be responsible for investigating into possible contraventions of the PDPA and data breaches involving personal data.

Where AI is used to generate content (eg, text, images) – if the content output from the AI system is false, toxic (eg, it incites racial or religious violence), or otherwise harmful to specific individuals or society at large (eg, deepfakes), action can be taken against the person who posted the generated content publicly under legislation such as the Protection from Online Falsehoods and Manipulation Act 2019, Protection from Harassment Act 2014, Maintenance of Religious Harmony Act 1990, Penal Code 1871, and Online Criminal Harms Act 2023.

HAS YOUR JURISDICTION PARTICIPATED IN ANY INTERNATIONAL FRAMEWORKS FOR AI?

Yes – some examples of the international frameworks for AI that Singapore has participated in include:

- the Bletchley declaration (November 2023), to promote the safety of AI and address frontier AI risks;
- developing the ASEAN Guide on AI Governance and Ethics (February 2024), together with the other nine ASEAN countries, to encourage alignment and interoperability of AI frameworks across the 10 ASEAN jurisdictions; and

developing the world's first AI Playbook for Small States (September 2024), together with Rwanda, and with input from more than 20 Digital Forum of Small States members, which sets out the challenges small states face in AI adoption and how these can be overcome.

WHAT HAVE BEEN THE MOST NOTEWORTHY AI-RELATED DEVELOPMENTS OVER THE PAST YEAR IN YOUR JURISDICTION?

There are three noteworthy developments in the areas of privacy, intellectual property and AI assurance or testing processes.

In relation to privacy, the PDPC had issued the 'Advisory Guidelines on the use of Personal Data in AI Recommendation and Decision Systems' in March 2024, following from its public consultation in July 2023. It clarifies how the PDPA will apply to the development and deployment of AI systems, with practical recommendations for organisations in areas such as how to obtain consent from individuals (when required).

In relation to intellectual property, the Intellectual Property Office of Singapore and the Singapore Management University issued 'When Code Creates: A Landscape Report on Issues at the Intersection of Artificial Intelligence and Intellectual Property Law' in February 2024. This landscape report sets out the position across various jurisdictions on key IP issues – such as whether there is copyright protection for AI-generated works, whether the use of works for machine learning infringes copyright, and whether an AI-generated work can infringe IP rights. While it does not set out a definitive position for Singapore as each case would turn on its facts, it helps readers site where Singapore's laws (and caselaw) stand among those internationally.

Finally, Singapore has expanded its AI system testing capabilities. AI Verify, when first launched, was a governance testing framework and software toolkit that could validate the performance of traditional AI systems against 11 internationally accepted ethics principles, using a series of technical and process checks. Singapore has now expanded AI Verify with Project Moonshot in May 2024, which is an evaluation toolkit for Large Language Models (LLMs). Project Moonshot offers benchmarks to test the LLM application across a variety of competencies such as language and context understanding, and also has facilities for manual and automated red-teaming to stress-test the LLM application to induce it to behave in a way that is incongruent with its design.

WHICH INDUSTRY SECTORS HAVE SEEN THE MOST DEVELOPMENT IN AI-BASED PRODUCTS AND SERVICES IN YOUR JURISDICTION? ARE THERE ANY EMERGING INDUSTRY OR NON-GOVERNMENTAL STANDARDS GOVERNING THE DEVELOPMENT AND USE OF AI-RELATED TECHNOLOGIES?

There is strong interest across all industry sectors in Singapore to harness AI in their day-to-day operations. AI is being used in healthcare, retail, education, manufacturing, financial services, legal services, defence, border control, etc. The government is also helping organisations to harness AI in their operations – for example, A*STAR (a statutory board) and the Ministry of Trade and Industry have recently set up a centre to assist the manufacturing sector in customising AI models to suit their needs.

AI Singapore (a multi-stakeholder partnership between various economic agencies in Singapore and academia) participates in international standard setting bodies. It has

contributed to the development of two standards: (1) ISO/IEC TR 24030:2021 Information Technology – Artificial Intelligence (AI) – Use Cases (note: a 2024 version is now available); and (2) Singapore Standards TR 99:2021 Artificial Intelligence (AI) security – Guidance for assessing and defending against AI security threats.

ARE THERE ANY PENDING OR PROPOSED LEGISLATIVE OR REGULATORY INITIATIVES IN RELATION TO AI?

Singapore's National AI Strategy 2.0 states that it is important that we 'retain agility' and take a 'pragmatic' approach to regulating the use of AI – '[t]he Government will take differentiated approaches to managing risks to and from AI, ranging from regulatory moves to voluntary guidelines, recognising that AI will continue to evolve.' There are no public plans yet to enact omnibus AI legislation similar to the EU or Canada.

We anticipate that there will be more guidelines issued by the various sectorial regulators in relation to the use of AI, where these will first be the subject of a public consultation to obtain views from the industry on whether they can be implemented and if they help to address the challenges faced by the industry.

WHAT BEST PRACTICES WOULD YOU RECOMMEND TO ASSESS AND MANAGE RISKS ARISING IN THE DEPLOYMENT OF AI-RELATED TECHNOLOGIES, INCLUDING THOSE DEVELOPED BY THIRD PARTIES?

There are several types of risks that arise from the use of AI – ranging from risks to fundamental rights (eg, discrimination, manipulation and loss of privacy), to safety risks (eg, death, injury, property damage) – where the risks are of different severity depending on the circumstances. However, the following best practices when developing or using an AI system can reduce the likelihood of these risks occurring:

- AI systems work based on probability, so there is always a chance that the output can be wrong. Therefore, it is important to have a level of human review before the output is implemented. However, we understand that it is not practical in all circumstances to have a human review the output (eg, in the case of high-speed financial trading), so organisations should consider the guidance in the Model AI Governance Framework, balancing the probability of harm against the severity of harm. Other factors to take into account would be the nature of the harm (whether physical or intangible), and whether the harm is reversible.
- In the same vein, it is important to know the limitations of the AI system and what its intended use is, and not to use it for other purposes as that will affect the quality or accuracy of its output. Employees should be trained on how to use the technology, including how it is expected to behave during normal use, and when to report incidents to management. Just as there are Standard Operating Procedures (SOPs) when a process is done by humans, SOPs should also be created when integrating AI into the same process.
- When you input confidential data (eg, personal data, or sensitive business data) into the AI system, whether to train the system, or when the system is deployed for the system to give an output in relation to the data, it is important to check with the system provider who can see the data input, where the data is stored, and whether the data will be used to further train the AI system. This is especially since there

have been cases of LLMs being subject to adversarial attacks and they then disclose confidential data they were trained on.

Insofar as using a third party's data to train your AI system may infringe their intellectual property rights, it would be the safest to obtain a licence or consent from anyone whose data you use. It is possible to rely on exceptions to copyright infringement in our Copyright Act 2021, namely the fair use exception and computational data analysis exception, but the scope of these exceptions are still untested in our local courts. Similarly, if a third party is developing an AI system for you, and using data from their own sources, you should obtain warranties and indemnities from them in relation to their rights to use that data.

The Inside Track

WHAT SKILLS AND EXPERIENCES HAVE HELPED YOU TO NAVIGATE AI ISSUES AS A LAWYER?

The first is to be curious about the technology and try it for ourselves. We test out the AI applications available to form our own views about them.

The second is to understand how AI works, and we rely on both our firm's in-house cybersecurity and privacy engineer as well as external resources such as videos for a 'behind-the-scenes' perspective.

The third is to read widely to be updated on AI developments locally and internationally. We read not only news articles and regulatory materials, but also academic commentary and reports from think-tanks, to get the most rounded perspective.

WHICH AREAS OF AI DEVELOPMENT ARE YOU MOST EXCITED ABOUT AND WHICH DO YOU THINK WILL OFFER THE GREATEST OPPORTUNITIES?

We look forward to how generative AI can be used to improve efficiencies in the workplace. While there is the issue of hallucinations, developers are working on many ways to reduce this issue, such as using retrieval-augmented generation, and building in features where the generated text can be cross-checked against the source text.

With proper guardrails built into a generative AI system, as well as training for individuals on how to use it, this technology can help with everything from idea-generation to analysing data to helping to sharpen arguments to support a client's case.

WHAT DO YOU SEE AS THE GREATEST CHALLENGES FACING BOTH DEVELOPERS AND SOCIETY AS A WHOLE IN RELATION TO THE DEPLOYMENT OF AI?

The risk of misinformation. Hallucinations produced by Large Language Models can be hard to detect, especially when they are not 'obviously' wrong, and very convincingly written. There is also the proliferation of deepfake images and videos (which look more realistic as the technology develops, and may not be labelled as AI-generated), making it difficult for people to tell whether what they are seeing is real or not. Our society must have new methods and tools to verify the authenticity of the content we consume, and everyone – society, developers and regulators – must work together on public education.

DREW & NAPIER

Lim Chong Kin	chongkin.lim@drewnapier.com
David N Alfred	david.alfred@drewnapier.com
Anastasia Su-Anne Chen	anastasia.chen@drewnapier.com
Cheryl Seah	cheryl.seah@drewnapier.com

Drew & Napier LLC

Read more from this firm on Lexology