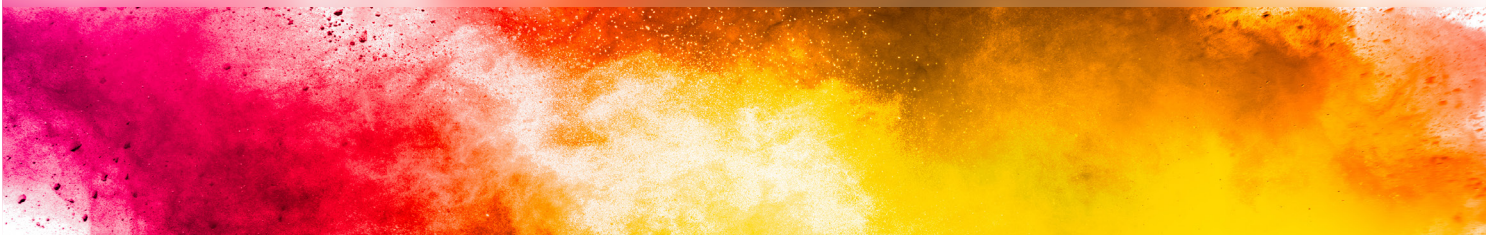


C L I F F O R D

C H A N C E



AI: THE EVOLVING LEGAL LANDSCAPE IN APAC

AI: THE EVOLVING LEGAL LANDSCAPE IN APAC

Asia Pacific (APAC) is a first mover in relation to AI regulation. Mainland China, in particular, has had city or regional regulations in place for some time and, more recently, enacted national AI regulations targeted at particular types of AI services or use. Across APAC, however, approaches vary significantly in relation to regulating AI. This article explores AI-related legislative developments across APAC, as part of our APAC tech themes series.

The Global AI Regulatory Landscape

We are seeing powerful advances in AI and machine learning – including the introduction of generative AI with an apparent ability to create and personalise. Synergies with other developing technologies, such as neurotechnology and quantum computing, are expected to further expedite AI developments. This presents both vast opportunities and a range of legal, ethical, and practical challenges. Organisations exploring AI opportunities are navigating a patchwork of overlapping law and, in some cases, sector-specific regulation, as they develop their AI strategies within their broader ethical, compliance and risk frameworks.

This landscape is evolving as governments globally consider whether to adapt existing legal frameworks to better address AI, with some countries developing AI-centric legislative and regulatory frameworks.

A watershed moment will be the promulgation of the EU's AI Act, which is expected shortly. It will be a key milestone in the evolving approach to regulating AI in the EU and beyond, introducing a risk-based framework for AI governance across the AI supply chain, with application beyond the EU and serious penalties (for more, see our article: [The EU's AI Act: What do we know about the critical political deal?](#)). The EU's AI Liability Directive is also being negotiated to introduce harmonising measures on civil liability and compensation for damage caused by AI.

In the US, the federal government is taking its first steps to advance a comprehensive framework for AI, with President Biden's [Executive Order on the Safe, Secure and Trustworthy Development and Use of AI](#) (EO), issued in October 2023. While the EO is primarily directed at government agencies, it is expected to shape regulation of private enterprises and industry best practice. (For more information see our articles: [What businesses need to know \(for now\) about the Biden Executive Order on AI?](#) and [Biden Executive Order on AI: what businesses can do \(for now\) about the safety and security mandates](#).)

We are also seeing increased international cooperation in relation to developing AI regulation and guidance. As the Cyberspace Administration of China (CAC) states, "*The governance of AI, a common task faced by all countries in the world, bears on the future of humanity.*"¹

The first focus topic of the series examining data themes in APAC can be found [here](#). For more in-depth analysis of tech issues and developments across APAC, see our second edition of *A Guide to Technology Disputes in Asia Pacific*, available [here](#).

¹ Dewey Sim, South China Morning Post, *Belt and road forum: China launches AI framework, urging equal rights and opportunities for all nations*, 18 October 2023, <https://scmp.com/news/china/diplomacy/article/3238360/belt-and-road-forum-china-launches-ai-framework-urging-equal-rights-and-opportunities-all-nations>

Within this global landscape of evolving AI legal frameworks and regulatory enforcement, developments across the APAC region showcase a range of strategic approaches in addressing AI-related challenges. In these jurisdictions the approach ranges from steadily putting in place targeted rules and regulations for AI in Mainland China to, at the other end of the spectrum, reliance on existing laws overlaid with sectoral and subject area guidance from key regulators (such as in Hong Kong and Singapore). Somewhere in between sit Japan and Australia, with their governments considering passing AI-specific legislation and conducting public consultation exercises, but in the meantime relying on adjusting existing law or supplementing it with high-level ethical principles and regulatory guidance. The common theme appears to be that APAC governments are closely monitoring the fast-evolving developments in AI and maintaining an agile approach. In this article we examine in more detail the AI-related legislative developments in Mainland China, Hong Kong, Singapore, Japan and Australia.

Emergence of legal architecture for AI in Mainland China and position in other APAC jurisdictions

Mainland China

The PRC has steadily been putting in place rules and regulations to ensure responsible use of AI, including regulations applicable to the production of ‘deepfakes’, provisions on recommendation algorithms and, most recently, measures governing generative AI service provision. Currently, the regulatory approach is agile and targets specific areas or uses of AI where lawmakers consider this to be necessary. This approach also means that the legislative landscape tends to be fragmented and overlapping, although the concepts underlying the regulation may be similar.

Generative AI:

- **The GenAI Measures:**

- In August 2023, the PRC cyberspace security and internet content regulator (CAC) released provisional measures targeting content generation (including the generation of text, images, audio and video content) using generative AI (the GenAI Measures). The GenAI Measures apply to any person that utilises generative AI technology to provide services to the public in Mainland China. As well as applying to those directly providing generative AI services, those indirectly providing services through programming interfaces and APIs are also captured. When considering the potential impact of the GenAI Measures, businesses should also beware of the Personal Information Protection Law (PIPL), the extra-territorial effect of which is triggered if the behaviour of individuals in Mainland China is being analysed and assessed. (For more on the PIPL, see our briefing [PRC Passes Milestone Legislation for Personal Information Protection](#).)

- The GenAI Measures seek to address issues such as quality of training data; data privacy and intellectual property protection; fraud prevention; discrimination and bias; accuracy; algorithmic transparency; security, governance and content moderation. The GenAI Measures provide that generative AI service providers must optimise algorithms to prevent the generation by AI of inappropriate content (for example, content endangering national security or content that is inconsistent with societal morals, as well as that which is discriminatory or inaccurate). Generative AI service providers are required to suspend or terminate services if such content or other improper use of the technology is discovered. Service providers capable of mobilising or influencing social viewpoints or public opinion are also required to complete a CAC security assessment, and be ready to respond to relevant regulators in relation to the source of the training data used and the algorithms and technical systems adopted. A

service agreement must be put in place between the providers and users of generative AI services, and a complaints-handling procedure must be established by the generative AI service provider. (For further details, see our briefing [China Moves to Further Regulate Artificial Intelligence: What Business Should Know](#) and Talking Tech article [China publishes Provisional Administrative Measures for Generative Artificial Intelligence Services](#).)

- The GenAI Measures also require the tagging or labelling of generative AI-created content (whether in the form of text, images, audio or video). Practical guidelines for such tagging or labelling were released by the NISSTC (a government standards setting body of which one supervisor is the CAC) in August 2023. The guidelines require generative AI service providers to tag or label relevant content with “Generated by Artificial Intelligence”, “AI-Generated” or similar by way of prompt text or “explicit watermark”, with further requirements in certain areas - such as specific rules regarding how visual content is labelled and requirements for metadata associated with saved or exported files.
- **The NISSTC draft security requirements for generative AI service providers:** The NISSTC released an exposure draft of security requirements for generative AI service providers for public consultation in October 2023, aimed at facilitating the practical implementation of the provisional measures. The draft security requirements deal with, among other things, the source of training data; AI model security or safety (specifically, the accuracy and reliability of content generated and model transparency); wider security or safety measures (this encompasses various aspects of safety such as protection of minors and AI-generated content labelling and moderation) and security assessment.

It is proposed that AI service providers be required to appoint responsible persons to deal with intellectual property issues including identifying and preventing services being provided based on infringing training data and establishing a mechanism to receive and handle infringement complaints. It is also proposed that they must not use personal data unless consent has been obtained (written consent is required in the case of biometric data) or another legal basis for use can be established. Service providers are to possess proof of the origin and legality of source data used to train the AI model. Also targeted towards protection of personal data, users should have the option of disabling the inclusion of their inputs for training. Service providers would be required to identify keywords and test questions (including a pool of test questions which would be rejected) to ensure illegal or undesirable content such as discriminatory content is not generated – with the classes of illegal or undesirable content of concern set out in an appendix to the security requirements. Requirements for security assessment are set out, including that these may be conducted by third-party agents. The security assessment results and supporting evidence should be filed with the application to begin providing services with relevant regulators. Security assessments should also be conducted for significant updates.

Other limbs of the PRC’s emerging AI framework include:

- **Regulating deepfakes.** The PRC has introduced regulation on deep synthesis data and technology², which took effect in January 2023. The relevant provisions target illegal activity – such as the production and dissemination of false news – which endangers national security or infringes others’ rights. It regulates deep synthesis service providers, technical support and users.

² Deep synthesis technology is defined in the provisions as technology using generative and/or synthetic algorithms such as deep learning or virtual reality to produce text, graphics, audio, video or virtual scenes

It covers requirements for verification of user identity; establishment of processes to recognise illegal or harmful information produced from deep synthesis technology and to deal with users who have produced such content (including appropriate platform conventions and service agreements, record-keeping, and reporting to relevant authorities); protection and security of training data including personal data; regular review of the algorithms used; the addition of a mark to enable identification of synthesised content; and security assessment requirements for tools used for generating or editing biometric data or information involving national security or public interests, and for products involving public opinion gathering or having social mobilisation ability.

- **Rules on recommendation algorithms.** Provisions on managing recommendation algorithms came into effect in Mainland China in March 2022. The provisions apply to any entity that uses algorithm recommendation technologies to provide internet information services within Mainland China.

The application is broad to cover services involving: (1) product and service personalised recommendation, for example, in online shopping and social media; (2) content generation, for example, in gaming and virtual environments; (3) sorting and ranking of search results; (4) filtering out of certain search results based on user needs or legal requirements; and (5) scheduling and resource allocation, for example, in ride-hailing, logistics or food-ordering applications. These service providers are required to ensure the fair and ethical use of such technology. This includes requirements to establish management systems and technical measures for user registration, data protection, security assessment and emergency response; content moderation; and combating fraud. Such service providers must also regularly review and evaluate their algorithms, data, and the results, and disclose to users the recommendation algorithm rules adopted and circumstances of use. Certain user rights have also been established including the right to opt out; to deletion of user tags targeting their personal characteristics; and not to be subject to differential treatment.

- **Ethical principles and related measures.** The PRC introduced national level guidance in the form of Opinions on Strengthening the Governance of Scientific and Technological Ethics in March 2022. The guiding tenet is enhancement of human well-being with the opinions requiring fairness, transparency and the establishment of an ethics review committee for organisations engaged in certain activities, specifically in the areas of AI, as well as life sciences and medicine. To supplement these principles, the Measures for Science and Technology Ethics Review were issued in September 2023 and became effective in December 2023.

The measures stipulate that the following scientific and technological activities are subject to ethics review: (1) scientific and technological activities involving the participation of human beings or use of experimental animals; and (2) other scientific and technological activities that may pose ethical risks in terms of, among other things, life, health and the ecological environment. The measures classify as high-risk the research and development of algorithm models, applications and systems with the ability to mobilise public opinion and guide social awareness, and of highly autonomous decision-making systems for scenarios that pose safety and personal health risks. Such research and development are subject to a second round of ethics review by the relevant local or industry department, unless exempted if the activity is already subject to administrative approval and regulatory requirements related to ethics.

Specific to financial institutions, the People's Bank of China correspondingly issued [Guidelines for Science and Technology Ethics in the Financial Sector](#) in order to steer ethical governance in the sector. By way of example to be adapted by organisations in light of actual needs, the National New Generation Artificial Intelligence Governance Professional Committee issued a model [code of ethics](#) in September 2021.

This AI regulation is against the background of the PRC calling for international public and private AI governance cooperation and equal rights to AI development by way of the Global AI Governance Initiative. As part of the initiative, the PRC also indicated its readiness to boost exchanges with other countries.

Hong Kong

To date, Hong Kong has relied on existing law and sectoral and subject area guidance from key regulators to deal with AI with the government closely monitoring evolving developments. There are signs, however, that the government is starting to take proactive action. Since May 2023, the Secretary for Innovation, Technology and Industry has taken the stance that the Internet is not an unreal world beyond the law – most of the existing laws enacted to prevent crimes in the real world are in principle applicable to the online world. He also referred to existing guidance from the PCPD (Hong Kong's data privacy regulator) for the ethical development and use of AI. In his most recent [response](#) to a question regarding AI in the Legislative Council (Hong Kong's legislature) in January 2024, the Secretary repeated this line and indicated that the AI guidance by the PCPD would be reviewed and updated as appropriate, but highlighted two areas into which the government was looking: (i) the government has commissioned the InnoHK research centre to study and suggest appropriate rules and guidelines covering the accuracy, responsibility and information security aspects of AI technology and its application; and (ii) the government is studying the copyright issues arising from the development of AI technology such as infringement issues from use of others' copyright for training and will conduct a consultation in 2024 to further explore enhancement of the existing protection provided by the Copyright Ordinance. Whilst we await these developments, we discuss the AI guidance from key regulators currently applicable in Hong Kong.

For more on some of the risk-mitigation measures that can be taken by financial services firms in relation to AI, see our Talking Tech article [here](#).

Guidance from the data privacy regulator

The PCPD calls for companies to review and critically assess the implications of any AI system on data privacy and ethics and, in particular, to follow the [Guidelines on the Ethical Development and Use of Artificial Intelligence](#) issued in August 2021. The guidelines refer to internationally recognised AI ethics principles including accountability, human oversight, transparency and interpretability, fairness, and data privacy, as well as reliability, robustness, and security.

In terms of practical steps to mitigate privacy risks, the PCPD suggests, as appropriate, collecting only the data that is relevant for AI use and development and discarding that which is irrelevant; using anonymised data (removal of identifiers of data subjects), pseudonymised data (replacement of identifiers of data subjects with other values) or synthetic data (which is artificially generated and does not relate to real people) to train AI; applying a differential privacy approach (usually "adding noises" through minor alterations) before release of a dataset to train AI; using a federated learning approach (developing AI models by separate computer systems each using only the data in the system so that the training data is never contained in a central database with only the trained AI models transferred out to further develop a consolidated and shared AI model); erasing personal data once it is no longer required; and a fair and transparent data collection policy.

More recently, in April and June 2023, the PCPD, in a [local newspaper article](#) and [article for the Hong Kong Lawyer](#), stressed the privacy concerns arising from the use of generative AI, whilst at the same time recognising its potential. The PCPD also highlighted that AI developers have a responsibility to ensure the data security of their AI systems in its [“Hong Kong Letter” publication](#) entitled “Artificial Intelligence is a Double-Edged Sword. Tech Firms are Duty-Bound to Ensure Data Security”.

Guidance from the securities regulator

In the financial services sector, a [speech](#) by the Head of Intermediaries of the Securities and Futures Commission (SFC) at the Web3 Festival in April 2023 emphasised that generative AI, as a novel technology, has its own limitations and flaws and therefore, the importance of harnessing its benefits in a responsible way. The CEO of the SFC had this to say regarding generative AI at the Hong Kong Investment Funds Association annual conference in June 2023: *“As a regulator, the SFC is guided by our philosophy to promote the responsible deployment of technology ... firms must ... make sure clients are treated fairly. We expect licensed corporations to thoroughly test AI to address any potential issues before deployment, and keep a close watch on the quality of data used by the AI. Firms should also have qualified staff managing their AI tools, as well as proper senior management oversight and a robust governance framework for AI applications. For any conduct breaches, the SFC would look to hold the licensed firm responsible – not the AI.”*

The SFC had earlier published Guidelines on Online Distribution and Advisory Platforms in July 2019, dealing with the use of AI in the context of online distribution of investment products and “robo advice” (namely, automated investment advice).

The guidelines similarly require licensed corporations to provide sufficient information to clients on how key components of their services are generated such as how underlying algorithms operate, and the limitations and risks involved; to properly and effectively manage and supervise development, operation and testing of algorithms used in digital advice tools; and to ensure adequate staff with sufficient expertise and understanding of the technology. An earlier SFC circular on algorithmic trading published in December 2016 also emphasised the importance of management and control function input in algorithmic governance.

Guidance from the banking regulator

The Hong Kong Monetary Authority (HKMA) published in November 2019, a circular regarding High-level Principles on AI and Guiding Principles on Consumer Protection in respect of Use of Big Data Analytics and AI by Authorised Institutions.

The principles set out are consistent with global themes for responsible use of AI including boards and senior management being accountable for AI-related outcomes; banks being required to ensure the explainability and ongoing monitoring of AI applications for producing fair and ethical outcomes; and the use of good quality data together with the safeguarding of personal data. Relatedly, after a thematic examination of algorithmic trading (which may or may not involve AI), the HKMA published guidance in March 2020 which, in addition to reiterating the need for proper governance and regular review of algorithms, also discussed requirements for robust pre-trade controls such as risk limits and tolerance, proper ‘kill’ functionality to suspend trading, business continuity and incident handling, and proper documentation. More recently, in April 2022, the HKMA issued the Regtech Adoption Practice Guide for AI-based Regtech Solutions. Again, the importance of establishing proper governance over AI and organisation data was highlighted. In January 2024, the PCPD published an article in *Banking Today*, a journal of the Hong Kong Institute of Bankers, entitled “AI and Ethics: Ensuring the Responsible Use of Generative AI in Banking”. The article highlighted the privacy and ethical concerns presented by generative AI and recommended following the Guidelines on the Ethical Development and Use of Artificial Intelligence published by the PCPD and the adoption of an appropriate personal data privacy management programme.

Guidance from the insurance regulator

The Insurance Authority (IA) considered how the current regulatory framework applies to AI chatbots in its periodical newsletter [Conduct in Focus](#) ([May 2023 issue](#)).

In terms of licensing the use of a chatbot in the insurance process, the IA cited the potential application of its Guideline on Enterprise Risk Management (GL 21), Guideline on Cybersecurity (GL 20) and Guideline on Outsourcing (GL 14). The IA emphasised the need for comprehensive testing under tight governance controls before deployment; clear disclosure of the chatbot's limitations, how it is to be used, the dataset on which it is trained, and how data is stored and used and how long it is to be retained; adequate risk mitigation; ongoing monitoring; and reporting controls and contingency plans. The IA emphasised an insurer or insurance intermediary's responsibility for a chatbot's output, and their overarching conduct and ethics requirements (including treating customers fairly and corporate governance requirements in the Code of Conduct).

Singapore

In Singapore, the financial and data regulators have issued soft law in a manner similar to Hong Kong. In addition, they have worked to develop practical tools to test and thus facilitate compliance.

Guidance (and methodologies to assess compliance) from the financial services regulator

In November 2018, the central bank and integrated financial regulator of Singapore (MAS) introduced fairness, ethics, accountability and transparency (FEAT) [principles](#) for the responsible use of AI and data analytics in the provision of financial products and services. Veritas Consortium (a MAS-led consortium comprising industry players) has since released [white papers](#) (in February 2022) providing for methodologies to assess compliance with FEAT principles.

These include: (i) FEAT checklist for AI software development and lifecycle; (ii) fairness assessment methodology to define fairness objectives, identify individual personal attributes and any unintentional bias; (iii) ethics and accountability assessment methodologies to quantifiably and qualitatively measure ethical practices; and (iv) transparency assessment methodology to determine how much internal and external transparency is needed to explain and interpret the predictions of machine learning models. The Veritas Consortium has also developed an [open-source software toolkit](#) to enable the automation of fairness metrics assessment.

Guidance (and governance testing framework) from the data privacy regulator

In January 2019, a Model AI Governance Framework (Model Framework) was issued by the Singapore Personal Data Protection Commission (PDPC) (with a [second edition](#) issued in January 2020) setting out voluntary guiding principles and practical measures for organisations seeking to deploy AI at scale focussing on internal governance; the appropriate level of human involvement in AI-augmented decision-making; operations management; and stakeholder interaction and communication. The PDPC also issued companions to the Model Framework in the form of [Implementation and Self-Assessment Guide for Organisations](#) and a [Compendium of Use Cases Volume 1](#) and [Volume 2](#) that show how local and international organisations across different sectors implemented or aligned their AI governance practices with the Model Framework. Following this practical guidance on implementing responsible AI, in May 2022, the PDPC and the Infocomm Media Development Authority (IMDA) went on to launch [AI](#)

Verify, an AI governance testing framework and toolkit to enable AI system developers / owners to be transparent and demonstrate responsible AI in an objective and verifiable manner.

Through the toolkit, comprising technical and process checks (including open-source testing solutions), AI system developers / owners are able to self-assess and verify claimed performance of their AI systems by way of standardised tests. The toolkit does not define ethical standards, but validates developers / owners' own claims. It allows testing on a common basis and generates reports for use by developers / owners as well as management and business partners.

In addition to the Model Framework, the PDPC also collaborated with others to launch A Guide to Job Redesign in the Age of AI, which provides industry-neutral and practical guidance to organisations to assist with their management of AI's impact on employees and redesign of existing jobs to increase their value and harness the potential of AI. The guidance recommends a human-centric approach including facilitating effective communication between employers and employees and encourages investment in the reskilling of employees.

Given the rapid advances in AI in the form of platforms and architecture such as ChatGPT and GPT-4, there has been an increasing need for guidance in this specialised domain.

In July 2023, the PDPC issued for consultation proposed Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems to address these advances in AI. Whilst the proposed guidelines will not be legally binding, they indicate how the PDPC will interpret statutory personal data obligations in the context of development and deployment of AI systems.

The guidelines reiterate that exceptions to the need for consent to use personal data in AI systems might be available in the form of the business improvement and research exceptions. In terms of existing notification for consent and accountability obligations, the guidelines state that where personal data is used in AI systems, organisations are encouraged to notify the functions of their AI product, the types of personal data that will be collected and processed, and how the collection and processing is relevant to the product feature in question. Organisations are also encouraged to provide information on their responsible data handling including data quality and governance measures. The proposed guidelines also deal with engagement of service providers for AI development and/or deployment.

More recently, in January 2024, the IMDA (in collaboration with the AI Verify Foundation) published for consultation the proposed Model Governance Framework for Generative AI, which builds on the Discussion Paper on Generative AI: Implications for Trust and Governance issued in June 2023 and the Model Framework published in January 2020 that had been based on traditional AI. The discussion paper in June 2023 highlighted that whilst generative AI involves some of the same risks as traditional AI, new issues have been raised such as hallucination, copyright infringement and misalignment with human values. Taking into account these risks, the framework seeks to set forth a "systemic and balanced approach" to address generative AI concerns while continuing to facilitate innovation.

In this regard, the framework provides meaningful guidance regarding the use and deployment of generative AI in the following nine dimensions: (i) accountability; (ii) source and quality of data; (iii) trusted development and deployment including

through transparency; (iv) incident reporting structures and processes; (v) third party testing and assurance; (vi) security; (vii) signalling to end users the provenance of AI-generated content including through technical solutions such as digital watermarking and cryptographic provenance; (viii) safety and value alignment research and development; and (ix) AI for the public good going beyond risk mitigation. Crucially, the framework emphasises the need for stakeholders involved in the development of generative AI to take responsibility based on their level of control. The consultation by IMDA and AI Verify Foundation seeks views from the international community whilst advocating global cooperation on policy approaches in order to harness the power of AI for the public good.

A further initiative in the form of a generative AI evaluation sandbox was launched by the IMDA and AI Verify Foundation in October 2023. The sandbox will make use of an Evaluation Catalogue, providing a common baseline of evaluation testing methods and benchmarks to assess generative AI products. The aim is to build up a body of knowledge of how generative AI products should be tested and develop new tests and benchmarks through collaboration with industry.

For more on AI Verify and Singapore's approach of developing standards and technical tools to ensure safety in digital development, see our Talking Tech article [Singapore to shape the future of international standards and unveils masterplan on digital infrastructure](#).

Japan

Japan has no AI-specific legislation. However, statutory AI regulation may be established in the future. In May 2023, the AI Strategic Committee (a public panel of experts) issued a Preliminary Screening of Issues regarding AI (the Preliminary Screening). The committee points out that compliance with existing laws and guidelines (through risk assessment and governance) should be encouraged. However, where it is impossible to solve the issues under existing legislation, the government and relevant stakeholders should consider taking appropriate measures.

The issues raised in the Preliminary Screening include: (i) the leakage of confidential information and other improper use of personal information; (ii) the potential to facilitate sophisticated crime; (iii) AI hallucinations; (iv) the sophistication of cyberattacks; (v) the use and potential misuse of generative AI in education; (vi) copyright infringement and (vii) the potential to increase unemployment. Further discussion and policymaking are expected in due course.

The government does currently have an AI strategy (first published in June 2019 and updated from time to time). The latest version (issued in April 2022) sets out five strategic goals: (i) to be able to deal with imminent crises such as pandemics and large-scale natural disasters through strengthening resilience; (ii) to develop and attract human resources; (iii) to enhance application in industry and industrial competitiveness; (iv) to establish technology and social systems to realise a sustainable development goals; and (v) to build international networks for research and development, and cooperation.

High level principles.

- **Social Principles.** In terms of high level ethical standards, the Japanese government published principles for implementing AI in society in March 2019, known as the [Social Principles of Human-Centric AI \(the Social Principles\)](#). The aim of the principles is not to restrict the use of AI, but to ensure human dignity, diversity and inclusion, and sustainability through AI.

The seven principles covered are: (i) human-centric (not misusing AI or infringing fundamental human rights and being responsible for the consequences of use); (ii) education / literacy to ensure the proper use of AI (iii) personal data and privacy protection; (iv) ensuring security, and properly assessing and managing risks; (v) fair competition; (vi) fairness, accountability and transparency; and (vii) innovation. The Ministry of Economy, Trade, and Industry (METI) further issued [Governance Guidelines for Implementation of AI Principles](#) in July 2021 (amended in January 2022), which discuss establishing an agile AI governance framework in collaboration with stakeholders to implement the Social Principles, as well as setting action targets for such implementation, hypothetical examples of action targets, and practical examples for gap analyses (in relation to gaps in attaining AI governance goals).

- **AI Development.** For developers engaged in AI research and development (R&D), as well as data providers and users, the Japanese government has also published principles for AI R&D in the form of [AI Utilisation Guidelines](#). Whilst the emphasis of the guidelines is on AI development, the guidelines have been extended to data providers and users because AI may change its implementation and output continuously through learning in the process of utilisation. In addition, the National Institute of Advanced Industrial Science and Technology has issued a [Machine Learning Quality Management Guideline](#).
- **AI Business Operators.** In December 2023, the AI Strategic Committee, a governmental expert panel, published draft guidelines setting out AI governance requirements which will need to be complied with by both the private and public sector where they engage in AI-related business. The guidelines set out the requirements for three categories of AI business operators as follows: (i) developers, (ii) service providers, and (iii) users with an emphasis on use of traceable data and data protection; fairness and anti-discrimination; security and vulnerability countermeasures; transparency and provision of information to stakeholders; and record-keeping and documentation. Public comments are being sought and the final version of the guidelines are expected to be published in about March 2024.
- **Contracting for AI.** METI also published Contract Guidance on Utilisation of AI and Data in June 2018 (updated from time to time), which discusses legal and drafting issues when negotiating contracts for the development and utilisation of AI and data, as well as setting out model clauses. The guidance covers intellectual property rights; terms of use; data privacy and security; appropriate limitations of liability on the part of the vendor; and data provision, creation, sharing and cross-border transfers.

Financial services sector requirements.

The Financial Instruments and Exchange Act requires businesses engaging in algorithmic high-speed trading to register with the government, and establish risk management systems and maintain transaction records.

Digital Platforms

The Digital Platform Transparency Act imposes requirements on online malls, app stores and digital advertising businesses to ensure transparency and fairness in transactions with business users including the disclosure of key factors determining their search rankings.

For more on the regulatory landscape generally and future outlook, see our detailed briefing [Japanese law issues surrounding generative AI: ChatGPT, Bard and beyond](#), which also discusses the complex legal issues surrounding AI in the Japanese context including in relation to copyright, data privacy and liability for harm.

Australia

There is no dedicated legislative regime in Australia regulating AI, with the Australian government so far taking a soft-law, principles-based approach.

For example, voluntary [AI Ethics Principles](#) were published by the Australian Department of Industry, Science and Resources in 2019 (discussed further below).

That said, there is an increasing number of government publications considering and guiding the future development of AI regulation. For example:

- In the [2023-2024 Federal Budget](#), the government allocated AU\$41.2 million to, among other things, support small and medium enterprises' adoption of AI technologies for improvement of their business processes and increasing competitiveness. It launched a [Responsible AI Adopt programme](#) and extended the National AI Centre to ensure AI usage through the government programme is responsible, and this will thereby act as a form of AI governance.
- For AI technology not part of this programme, the government issued two publications, in March and June 2023, respectively, to begin a discussion to ensure appropriate safeguards are in place for the safe and responsible growth of AI technologies in Australia, which the industry minister has described as a “balancing act” and might involve banning high-risk activities such as the use of AI-enabled robots for medical surgery.
 - The first paper for public consultation, published by the Department of Industry, Science and Resources, is entitled [Safe and Responsible AI in Australia](#) and considers the existing governance and regulatory frameworks in Australia (through consumer protection, online safety, privacy and criminal laws) and internationally, and proposes options to strengthen the Australian framework for safe and responsible use of AI. The second report, published by the National Science and Technology Council, is entitled [Rapid Response Information Report: Generative AI and identifies potential opportunities and risks in relation to generative AI](#), as well as examples of international strategies to address such opportunities and risks, providing a scientific basis for discussions about the way forward. The publications do not consider all implications of AI, specifically neither intellectual property nor labour market implications.
 - In January 2024, the Australian government published an [interim response](#) to the discussion begun in 2023. The Australian government has indicated that based on submissions received and with broad public consensus, where there is use of AI in legitimate yet high risk settings, legislative mandatory guardrails will be considered whether through amendments to existing law (such as privacy and online safety laws) or through dedicated legislation. An expert advisory body will be established to consider the risks of AI. Specific obligations for the development, deployment and use of AI for general-purpose models are also being considered. Reference will be made to developments in other countries. The aim is to support the development of AI in Australia and ensure its use in low-risk settings is allowed to flourish. In this regard, a voluntary AI Safety Standard is being developed to facilitate industry being able to take a risk-based approach by referencing a single source, as opposed to the existing plethora of guidelines, which is practical and showcases best practice.
- In September 2023, the Australian Human Rights Commission's (HRC) made a submission to the United Nations Office of the Secretary-General's Envoy on Technology regarding “[Centring Human Rights in the Governance of Artificial Intelligence](#)”, which advocated for human rights to be a central consideration in the

global governance of AI. This followed the [HRC's 2021 Human Rights and Technology final report](#) which put forward a model for AI regulation in Australia that had its basis in human rights protection.

The HRC 2021 report recommended the creation of an independent statutory office, the AI Safety Commissioner, to provide expert guidance to and collaborate with legislators, government agencies and regulators to address risks and promote safety and protect human rights in the development and use of AI. Whilst such an office has yet to be created, with the Online Safety Act having come into force in January 2022, the national eSafety Commissioner (responsible for online safety) has been issuing [transparency notices](#) to recommender algorithm and system service providers to require them to report how they are meeting the [Basic Online Safety Expectations](#).

In September 2023, the eSafety Commissioner [registered](#) an industry code applicable to internet search engine service providers (to come into effect March 2024), which had taken into account the Commissioner's request to consider the integration of generative AI into search engine services and address associated risks of harm – including access to AI-generated child sexual exploitation, and terror, crime and violence – as material. The eSafety Commissioner also suggested in its [generative AI position statement](#) that its [Safety by Design](#) principles are applicable to AI, as they are applicable to any new online and digital technology. The Commissioner further suggested that the online industry can take a leading role in safeguarding user rights and fostering healthy innovation by adopting such principles.

Government use of AI

In terms of government use of AI, the HRC 2021 report recommended mandatory human rights impact assessments, notice of government use of AI, and that individuals subjected to government decisions made with AI have a right to reasons and recourse to an independent merits review. In September 2023, the [Federal Government announced an Artificial Intelligence in Government Taskforce](#), focused on the safe and responsible use of AI by the Australian Public Service.

AI Ethics Principles

The HRC 2021 report further encouraged private sector adoption of the AI Ethics Principles.

The [AI Ethics Principles](#) cover principles such as:

- Human-centred values, which provides that AI systems should respect human rights, individual autonomy, and diversity.
- Societal and environmental well-being, which provides that AI systems should benefit both society and the environment, and their impact throughout their lifecycles should be accounted for.
- Fairness, which provides that AI systems should be inclusive, accessible and not involve unfair discrimination.
- Privacy protection and security, which provides that AI systems should uphold privacy rights and ensure the protection and security of data.
- Transparency and explainability, which provides that there should be transparency and responsible disclosure so that people can understand AI's engagement and impact on them.

- Contestability, which provides that there should be timely processes to allow people to challenge the use and outcomes of AI systems where they are significantly affected.
- Accountability, which provides that there should be human oversight of AI systems and the people responsible should be identifiable and accountable for the outcomes of AI systems.

Privacy Law

To take into account the issues or risks arising from AI, the general law, such as data privacy law, has been modified. The Attorney General's Department published the [Privacy Act Review Report](#) in February 2023, proposing 116 changes to the existing Privacy Act. The Australian government released its [response](#) to the Report in September 2023. In short, the government agreed to 38 proposals and agreed in principle to 68 proposals.

Agreed in principle means that further engagement and comprehensive impact analysis will be carried out before the government decides on implementation of the relevant proposals. Further consultation and legislative proposal work will progress into 2024. The AI-related recommendations in the Report and consequent issues are summarised below. The Report recognises that these recommendations should be implemented as part of broader work by the Australian government to regulate AI.

- Explainability. In respect of direct marketing, entities will be required to provide information about targeting including clear information about the use of algorithms and profiling to recommend content to individuals (**proposal 20.9**). This would appear to require operators of AI systems to disclose the applicable principles (albeit not necessarily the logic) adopted by algorithms used to profile and recommend content to individuals. On the other hand, the proposed requirements for "substantially" automated decisions that have a legal or similar significant effect on individuals' rights will be more stringent, requiring disclosure of the types of personal information that will be used in such decision-making in privacy policies and how decisions will be made upon request (**proposal 19**). These requirements might lead to difficulties for AI system operators which themselves might not be entirely clear as to what information is used and how decisions are made due to the black box effect (in the majority of machine learning and deep learning models, the internal workings of the model in terms of the decision-making and learning process is not known even to the person who designed the model). The government has stated that it agrees in principle to proposal 20.9 and agrees to proposal 19. Regarding proposal 20.9, the government's main outstanding concern is to ensure meaningful information is provided to individuals. Regarding proposal 19, the government indicated that guidance will be given as to the type of decisions considered to have a significant effect on individuals' rights, with possible examples being denial of services such as financial and lending, insurance, housing, education, employment and healthcare services. The implementation of both proposals will be part of a broader consultation and other work to regulate AI.
- Fair and reasonable collection, use and disclosure of personal information, to be assessed on an objective standard, irrespective of consent (**proposal 12**). The policy rationale for this recommendation is fair trading. However, it might create difficulties for businesses using machine learning and deep learning, as the black box effect means they often do not have visibility as to the model's decision-making and learning and thus how personal information is being used or retained or whether its use or retention is reasonably necessary might not be known. The government has stated that it agrees in principle to proposal 12 and indicated that guidance will be given to "map the contours" of the fair and reasonable test including factors to be considered.

Practical steps for AI strategy development or enhancement

When identifying and exploring opportunities for the use of AI, having multidisciplinary teams involved to ask the right questions to support responsible, informed decision-making is crucial. The starting point is to map the use of AI, understand the legal frameworks and risks, and develop appropriate oversight principles and robust governance programmes to mitigate those risks. Organisations will also need to identify appropriate decision-makers, look at their wider governance structures and processes, and consider their AI-related communications. Although the legal landscape for AI is evolving – across APAC and globally – now is the time to develop AI legal and ethical strategies and risk-management frameworks.

For further insight into AI themes in APAC, see section 12 of our [Guide to Technology Disputes in Asia Pacific](#).

The Guide sets out some key issues arising from technology protection, regulation and disputes in Asia Pacific. Each section features a summary of the key issues and provides guidance on how companies operating in each of the jurisdictions highlighted should best protect and enforce their IP in a digital environment, protect their data and data privacy and handle cybersecurity incidents, and deal with a range of technology regulations and disputes, such as in the areas of AML, sanctions, anti-trust, fintech, responsible tech and product / contractual liability.

CONTACTS

HONG KONG



Ling Ho
Partner
Hong Kong
T: +852 2826 3479
E: ling.ho@cliffordchance.com



Charmaine Kwong
Senior Associate
Hong Kong
T: +852 2825 8992
E: charmaine.kwong@cliffordchance.com



Justin Luo
Registered Foreign Lawyer
Hong Kong
T: +852 2826 3488
E: justin.luo@cliffordchance.com



Felicia Cheng
Professional Support
Lawyer
Hong Kong
T: +852 2826 3526
E: felicia.cheng@cliffordchance.com

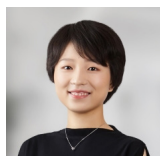


Clarice Yue
Counsel
Hong Kong
T: +852 2825 8956
E: clarice.yue@cliffordchance.com

MAINLAND CHINA



Lei Shi
Partner
Shanghai
T: +86 21 2320 7377
E: lei.shi@cliffordchance.com

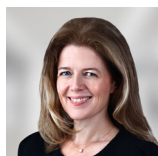


Jane Chen
Senior Associate
Beijing
T: +86 10 6535 2216
E: jane.chen@cliffordchance.com



Jessy Cheng
Associate
Shanghai
T: +86 10 6535 4935
E: jessy.cheng@cliffordchance.com

SINGAPORE



Stella Cramer
Partner
Singapore
T: +65 6410 2208
E: stella.cramer@cliffordchance.com



Janice Goh
Partner, Cavenagh Law
Singapore*
T: +65 6661 2021
E: janice.goh@cliffordchance.com

TOKYO



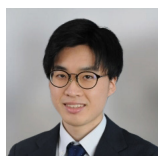
Joey Ng
Associate
Singapore
T: +65 6661 2059
E: joey.ng@cliffordchance.com



Peter Harris
Partner
Tokyo
T: +81 3 6632 6635
E: peter.harris@cliffordchance.com



Michihiro Nishi
Partner
Tokyo
T: +81 3 6632 6622
E: michihiro.nishi@cliffordchance.com

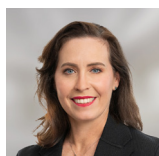


Masaya Obayashi
Qualified Lawyer
Tokyo
T: +81 3 6632 6370
E: masaya.obayashi@cliffordchance.com



Sian Smith
Senior Associate
Tokyo
T: +81 3 6632 6320
E: sian.smith@cliffordchance.com

AUSTRALIA



Naomi Griffin
Partner
Sydney
T: +61 2 8922 8093
E: naomi.griffin@cliffordchance.com



Robert Tang
Counsel
Sydney
T: +61 2 8922 8502
E: robert.tang@cliffordchance.com

*Cavenagh Law LLP and Clifford Chance Pte Ltd are registered as a formal law alliance in Singapore under the name Clifford Chance Asia.

C L I F F O R D

C H A N C E

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

Any advice above relating to the PRC is based on our experience as international counsel representing clients in business activities in the PRC and should not be construed as constituting a legal opinion on the application of PRC law. As is the case for all international law firms with offices in the PRC, whilst we are authorised to provide information concerning the effect of the Chinese legal environment, we are not permitted to engage in Chinese legal affairs. Our employees who have PRC legal professional qualification certificates are currently not PRC practising lawyers.

Cavenagh Law LLP and Clifford Chance Pte Ltd are registered as a formal law alliance in Singapore under the name Clifford Chance Asia. Please approach Cavenagh Law LLP if you require any advice on the Singapore litigation or criminal law aspects discussed in this publication.

www.cliffordchance.com

Clifford Chance, 27th Floor, Jardine House, One Connaught Place, Hong Kong

© Clifford Chance 2024

Clifford Chance

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.