

A YIN-YANG APPROACH TO BALANCED AI REGULATION AND LESSONS FOR SINGAPORE

Lao Tzu’s quote – “[a]ll things carry *yin* yet embrace *yang*. They blend their life breaths in order to produce harmony”¹ – carries lessons on striking the right balance for AI regulation in Singapore. For Singapore, which is a “fast follower” in the global AI race, the key is to learn lessons quickly from international precedents, while aligning with and influencing global developments to ensure interoperability. This article aims to demonstrate that Singapore should not seek to find a single “correct” point of balance. Instead, it should advance aspects key to building the groundwork for international AI governance – and in so doing, serve as a forward-looking model for how small states can ride the AI wave.

Josh LEE Kok Thong

LLB (Singapore Management University), LLM (University of California, Berkeley, School of Law);

Managing Director, Asia-Pacific, Future of Privacy Forum; Adjunct Faculty (AI Law, Policy and Ethics), Singapore Management University.

PANG Cheng Kit, Kit²

LLB (Singapore Management University);

Justices’ Law Clerk (Singapore).

I. Introduction

1 In many Asian cultures, the philosophy of *yin* and *yang* – and how a proper balance of both elements produces harmony – is a founding heuristic principle around which societies and aspects of life are organised. This philosophy views paradoxes as interdependent opposites, which is distinct from the general Western view of paradoxes as exclusive opposites.³ At first blush, this philosophy could not seem further removed

1 J Legge, J H McDonald & Lin Yutang, “Lao Tzu Tao Te Ching Chapter 42”, *Tao in You* <<https://tao-in-you.com/lao-tzu-tao-te-ching-chapter-42/>> (accessed 16 August 2025).

2 This article is written in the authors’ personal capacities, and the opinions expressed in this article are entirely the authors’ own views.

3 Tony Fang, “Yin Yang: A New Perspective on Culture” (2012) 8 *Management and Organization Review* 25 at 26.

from a topic like artificial intelligence (“AI”) governance and regulation. However, it lends a useful nuance to the central question of this paper: in light of continued technological progress, how should a small, yet highly globalised and technology-oriented nation like Singapore orient its AI governance and regulatory framework to balance the benefits and risks of AI?

2 As a nation seeking to position itself as a global technology hub, Singapore is confronted with the strategic need to promote technological innovation and adoption, while providing credible safeguards to preserve public trust in AI due to rising concern about issues relating to ethics, privacy, security, and accountability, among others. This article posits that for smaller jurisdictions like Singapore – which are recognised as “fast followers”⁴ rather than “first-movers” – an effective national AI governance and regulatory framework comes from learning relevant lessons quickly from international precedents, while aligning with and shaping global developments to ensure interoperability. This article also explores whether further tweaks to Singapore’s existing regulatory approach need to be made to ensure its longer-term viability and sustainability.

3 This article proceeds as follows: Paragraphs 4–34 first explore the foundational concepts of AI governance and regulation, highlighting key challenges and considerations that policymakers face. Paragraphs 35–48 delve into Singapore’s specific strategies and policies regarding AI governance. In particular, the section explores how Singapore leverages its position as a “fast follower” to implement regulatory initiatives that are fit-for-purpose while also defining international best practices. Paragraphs 49–83 provide a comparative analysis of AI regulatory approaches in the US, the European Union (“EU”) and China, as well as regulatory efforts at regional and global levels. Paragraphs 84–102 conclude by synthesising and applying the insights gained to Singapore’s regulatory model going forward.

4 Wong Pei Ting, “Nimble, Flexible, but with Guard Rails: DPM Gan Lays Out S’pore’s AI Approach at Davos Panel”, *The Straits Times* (22 January 2025) <<https://www.straitstimes.com/singapore/nimble-flexible-but-with-guardrails-dpm-gan-lays-out-singapores-ai-approach-at-davos-panel>> (accessed 15 December 2025).

II. Foundational concepts and considerations in artificial intelligence governance and regulation

A. *Balancing innovation and risk*

4 One word appears above all others in global AI governance and regulation parlance: balance. This balance refers to the need to develop governance and regulatory frameworks that balance the risks and rewards of AI:⁵ while AI brings with it significant benefits that can fundamentally transform society by greatly improving efficiencies and providing new capabilities, it is also inherently fraught with societal concerns and risks. The challenge is thus often framed as a balancing act between promoting technological advancement and imposing safeguards to keep AI's potential harms in check.⁶

5 The view that AI governance and regulation is about finding the right balance is, while not wrong, perhaps limited in utility. It recalls the image of a sliding scale: once the right balance is found through the right mix of regulatory and governance instruments, a jurisdiction can expect to reap maximal benefits while keeping AI's biggest harms at bay. Such an image also reflects a (perhaps Westernised) conception of balance being a matter of managing exclusive opposites.

6 A revised and more insightful view of AI governance and regulation may instead be to view innovation and safeguards not as a zero-sum game, but as a virtuous cycle of trust. This notion of a virtuous cycle of trust recalls the *yin-yang* conception of interdependent opposites, and is rooted in the idea of trusting digital technologies when they perform in the way society expects them to.⁷ In this sense, trust is

5 Paulo Carvão *et al*, *Governance at a Crossroads: Artificial Intelligence and the Future of Innovation in America* (M-RCBG Associate Working Paper Series No 251) (Mossavar-Rahmani Center for Business and Government, Harvard Kennedy School, 2025) at p 22 <https://www.hks.harvard.edu/sites/default/files/Final_AWP_251_2.pdf> (accessed 15 December 2025).

6 See Lim Fang-Zhou, Noah & Tan Kay Shin, "The New Frontier: Regulating Artificial Intelligence in Singapore" (2025) 37 SAclJ 436. See also Paulo Carvão *et al*, "Governance at a Crossroads: Artificial Intelligence and the Future of Innovation in America" (M-RCBG Associate Working Paper Series No 251) (Mossavar-Rahmani Center for Business and Government, Harvard Kennedy School, 2025) <https://www.hks.harvard.edu/sites/default/files/Final_AWP_251_2.pdf> (accessed 15 December 2025) and Jason Grant Allen, Jane Loo & Jose Luna, "Governing Intelligence: Singapore's Evolving AI Governance Framework" (2025) 1 *Cambridge Forum on AI: Law and Governance* e12 <<https://doi.org/10.1017/cfl.2024.12>> (accessed 5 January 2026).

7 See definition of "digital trust" in World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies* (Insight Report, November 2022) (*cont'd on the next page*)

a prerequisite for broader AI adoption: people and organisations will embrace AI-driven technologies if they feel relatively confident in them. At the same time, trust in AI grows through successful adoption and use. This creates a positive feedback loop: applying appropriate safeguards fosters public trust in AI and encourages its use, which in turn justifies and strengthens those safeguards.

7 With this in mind, the authors turn to two foundational realities that Singapore’s policymakers must reckon with in AI policymaking. The first reality is Singapore’s position as a small, open and highly interconnected city-state. This reality entails realising that Singapore cannot afford to succumb to the “ostrich effect”.⁸ In other words, it would neither be possible for Singapore to ignore developments in AI over the years, nor to artificially insulate itself from technological developments (such as banning the use of generative AI in the country). Therefore, regardless of the trajectory of AI development going forward, Singapore must always be ready to take the good with the bad, and to find ways of managing the double-edged nature of AI technologies.

8 A second foundational reality that must be appreciated is Singapore’s position in the ecosystem. Singapore is primarily a deployer state,⁹ as compared to the handful of jurisdictions (including the US, China, and to some extent, Europe) able to claim the mantle of primary developers of underlying AI technologies. Combined with Singapore’s small domestic economic market, this limits the degree of influence Singapore has in shaping or regulating how AI is developed at source. Given this, governance over AI must be done indirectly, focusing on how it is deployed within one’s borders. In global AI governance debates, these dynamics give rise to the notion of “deployer states” *versus* “developer states”.¹⁰ Deployer states (*ie*, the majority of jurisdictions

<https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf> (accessed 15 December 2025).

- 8 Niklas Karlsson, George Loewenstein & Duane Seppi, “The Ostrich Effect: Selective Attention to Loewenstein” (2009) 38 *Journal of Risk and Uncertainty* 95 <<https://www.cmu.edu/dietrich/sds/docs/loewenstein/OstrichEffect.pdf>> (accessed 15 December 2025).
- 9 Jason Grant Allen, Jane Loo & Jose Luna, “Governing Intelligence: Singapore’s Evolving AI Governance Framework” (2025) 1 *Cambridge Forum on AI: Law and Governance* e12 <<https://doi.org/10.1017/cfl.2024.12>> (accessed 5 January 2026). Singapore is described in this article as a “net importer” of technology, but the implication is the same: that rather than being a jurisdiction that primarily develops technology, it has to import and deploy them in a domestic context.
- 10 Philipp Hacker, Ramayya Krishnan & Marco Mauer, “Global AI Governance – Part 1: Decoding Developers and Deployers”, *Oxford Business Law Blog* (9 December 2024) <<https://blogs.law.ox.ac.uk/oblb/blog-post/2024/12/global-ai-governance-part-1-decoding-developers-and-deployers>> (accessed 15 December 2025).

globally) face the challenge of exerting influence over technology largely developed elsewhere.¹¹ This reality makes adaptable domestic policy and international co-operation crucial, since direct unilateral control over AI innovation is beyond reach for regulators in non-developer states.

9 Accordingly, global AI governance demands a multi-stakeholder approach.¹² No single entity – whether government, industry, academia, civil society or international organisation – can address AI’s sweeping impact in isolation.¹³ Governments provide oversight and public accountability, industry contributes technical expertise and resources, academic and research institutions offer analysis and guidance, civil society voices public values and concerns, and international organisations provide platforms for jurisdictions to engage in constructive discussion. Notably, international forums and alliances have stressed the importance of joint action: for example, the United Nations’ High-Level Advisory Body on AI,¹⁴ the Council of Europe’s Framework Convention on AI¹⁵ and other multilateral declarations emphasise that collective effort is crucial in “addressing the technology’s risks and capitalising on its opportunities”.¹⁶ In short, the fundamental nature of AI governance must, inherently, be co-operative. Effective regulation of AI should therefore be viewed as a team sport – one that, when played well, builds public trust and accelerates responsible adoption of AI innovations.

10 The following subsections explore several key policy and regulatory considerations that jurisdictions, including Singapore, need

-
- 11 Philipp Hacker, Ramayya Krishnan & Marco Mauer, “Global AI Governance – Part 1: Decoding Developers and Deployers”, *Oxford Business Law Blog* (9 December 2024) <<https://blogs.law.ox.ac.uk/oblb/blog-post/2024/12/global-ai-governance-part-1-decoding-developers-and-deployers>> (accessed 15 December 2025).
 - 12 United Nations, *Governing AI for Humanity: Final Report* (September 2024) at para 102 <https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf> (accessed 15 December 2025).
 - 13 United Nations, *Governing AI for Humanity: Final Report* (September 2024) at paras 41–45 <https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf> (accessed 15 December 2025).
 - 14 United Nations, *Governing AI for Humanity: Final Report* (September 2024) <https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf> (accessed 15 December 2025).
 - 15 Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (17 May 2025), Eur TS No 225 (opened for signature 5 September 2024) “Framework Convention on AI”. See in particular, Arts 19 and 25 of the Framework Convention on AI <<https://rm.coe.int/1680afae3c>> (accessed 15 December 2025).
 - 16 Cathy Li, “Responsible AI Governance Can be Achieved Through Multistakeholder Collaboration”, *World Economic Forum Stories* (14 November 2023) <<https://www.weforum.org/stories/2023/11/ai-development-multistakeholder-governance/>> (accessed 15 December 2025).

to consider when developing AI governance and regulatory policies. These areas are: (a) definitional and scope considerations; (b) regulatory approaches; (c) governance objectives and policy design considerations; and (d) implementation considerations.

B. Considerations of definition and scope

11 The very *definition* of “AI” remains contested globally.¹⁷ Ever since the term was coined in the 1950s, it has been a moving target – from rule-based expert systems to today’s machine learning models – and its boundaries remain hazy.¹⁸ This lack of consensus has real regulatory implications. Parties analysing and applying laws and regulations need to know what falls under “AI” and what does not.¹⁹ Yet, reaching a clear, lasting definition has proven inherently difficult. The term “AI” can evoke the image of human-like cognition, but it can also be casually applied to straightforward algorithms that would hardly seem intelligent to a layperson. Indeed, the Organisation for Economic Co-operation and Development (“OECD”) felt compelled to update its official definition of an AI system in 2023 to ensure its “continued relevance”²⁰ – illustrating how any static definition can quickly become outdated in this fast-changing field.

12 Most attempts to provide a universal definition on AI fall under either one of two definitional approaches.²¹ One approach – known as “human-centric definitions” – defines AI by reference to human

17 Daniel Seng, Jerrold Soh Tsin Howe & Lim How Khang, “An Introduction to the Relevant Technologies” in *Law and Technology in Singapore* (Simon Chesterman, Goh Yihan & Andrew Phang Boon Leong eds) (Academy Publishing, 2nd Ed, 2025) ch 2 at para 02.016.

18 Jacob Turner, “Introduction” in *Robot Rules* (Palgrave Macmillan, 2019) ch 1.3 at p 8: “Defining AI can resemble chasing the horizon: as soon as you get to where it was, it has moved somewhere into the distance.” See also Marko Grobelnik, Karine Perset & Stuart Russell, “What is AI? Can you make a clear distinction between AI and non-AI systems?”, *The AI Wonk* (6 March 2024) <<https://oecd.ai/en/wonk/definition>> (accessed 6 January 2026).

19 Jacob Turner, “Introduction” in *Robot Rules* (Palgrave Macmillan, 2019) ch 1.3 at p 9: “In short, people cannot choose to comply with rules they do not understand. If the law is impossible to know in advance, then its role in guiding action is diminished if not destroyed. Unknown laws become little more than tools of the powerful.”

20 OECD, *Explanatory Memorandum on the Updated OECD Definition of an AI System* (OECD Artificial Intelligence Papers No 8) (OECD Publishing, 2024) at p 4 <https://www.oecd.org/en/publications/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_623da898-en.html> (accessed 15 December 2025).

21 Jacob Turner, “Introduction” in *Robot Rules* (Palgrave Macmillan, 2019) ch 1.3 at p 9: “Most of the universal definitions of AI that have been suggested to date fall into one of two categories: human-centric and rationalist.”

intelligence.²² This approach describes AI as machines doing things “that require intelligence when performed by people”.²³ This anthropomorphic lens, while superficially appreciable at first, runs into two issues. Firstly, it begs the question of what is “human intelligence”, a concept that is itself deeply contested. Secondly, limiting AI systems to the level of human intelligence, even assuming there were consensus on what it meant, could be overly narrow: it might exclude systems that perform tasks no human could do (like analysing billions of data points in seconds) or label as “AI” only those machines that exhibit human-like cognition. Such definitions may miss forms of AI that are powerful but not particularly human-like in how they operate.²⁴ The other definitional approach focuses on autonomy or technical capabilities.²⁵ For example, defining AI as any system that can operate with some level of autonomy and generate outputs such as predictions or decisions. These capability-based definitions can often be over-inclusive, covering technologies that society does not actually perceive as “intelligent”. If interpreted too broadly, any autonomous decision-making software might count as AI, including relatively simple automated systems that do not warrant special treatment. The divergence in support for these two approaches is well-documented. For instance, a US Department of Defense strategy paper on AI adopts the human-centric view (defining AI as “the ability of machines to perform tasks that normally require human intelligence”)²⁶, whereas the OECD’s formulation describes a “machine-based system” that produces certain outputs (such as predictions, content recommendations and decisions).²⁷ Each captures part of the truth, and yet neither fully satisfies everyone.

22 Jacob Turner, “Introduction” in *Robot Rules* (Palgrave Macmillan, 2019) ch 1.3.

23 Ray Kurzweil, *The Age of Intelligent Machines* (MIT Press, 1992) ch 1.

24 Jacob Turner, “Introduction” in *Robot Rules* (Palgrave Macmillan, 2019) ch 1.3.

25 Matt O’Shaughnessy, “One of the Biggest Problems in Regulating AI is Agreeing on a Definition”, *Carnegie Endowment for International Peace Commentary* (6 October 2022) <<https://carnegieendowment.org/posts/2022/10/one-of-the-biggest-problems-in-regulating-ai-is-agreeing-on-a-definition?lang=en>> (accessed 15 December 2025). See also Jacob Turner, “Introduction” in *Robot Rules* (Palgrave Macmillan, 2019) ch 1.3.

26 US Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity* (2019) at p 5 <<https://nsarchive.gwu.edu/document/18393-national-security-archive-department-defense>> (accessed 15 December 2025).

27 OECD, *Explanatory Memorandum on the Updated OECD Definition of an AI System* (OECD Artificial Intelligence Papers No 8) (OECD Publishing, 2024) <https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/03/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_3c815e51/623da898-en.pdf> (accessed 15 December 2025).

13 The EU AI Act²⁸ provides an example of how regulators have wrestled with the issue of definitions.²⁹ The EU AI Act (adopted in 2024) defines an “AI system” as “a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.”³⁰ This EU definition is illustrative of a potential third definitional approach – one that is technology-neutral and future-proof. Such an approach avoids referencing specific techniques (no mention of neural networks, for example) and instead focuses on functional criteria (autonomy and the nature of outputs). By listing typical outputs (*eg*, predictions, recommendations, decisions, *etc*), the EU AI Act delineates its definitional scope without being tied to any single AI methodology. While not necessarily universally accepted, this definition may become a reference point for other jurisdictions, especially given the EU AI Act’s extraterritorial applicability.³¹

14 Beyond definitional wording, there is also the question of *scope*: what exactly should fall within the ambit of AI governance? Because AI governance extends beyond just covering software algorithms to the entire socio-technical ecosystem in which AI operates, rules must thus account for the human and institutional actors around the AI, and the relationships between them. For example, who develops the system? Who deploys it and in what context? Who is affected by its decisions? A holistic governance regime must consider issues like data provenance (*ie*, where training data comes from), the role of human oversight, and feedback loops between AI and society. As commentators have observed, paying attention to the broader context – rather than just the technical artefacts – is necessary to grasp how AI systems impact

28 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence [2024] OJ L 2024/1689 (“EU AI Act”).

29 See European Parliament, “Artificial Intelligence Act”, *Legislative Train Schedule* <<https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence>> (accessed 15 December 2025). See also Bernhard Nessler & Christiane Wendehorst, *Commission Guidelines on the Application of the Definition of an AI System and the Prohibited AI Practices Established in the AI Act* (European Law Institute, 2024) <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Response_on_the_definition_of_an_AI_System.pdf> (accessed 15 December 2025).

30 EU AI Act Art 3(1). See <<https://artificialintelligenceact.eu/article/3/>> (accessed 15 December 2025).

31 EU AI Act Art 2(1). See <<https://artificialintelligenceact.eu/article/2/>> (accessed 15 December 2025).

people and communities.³² In practice, this calls for mapping out the AI lifecycle and the ecosystem of stakeholders. Modern AI governance frameworks increasingly emphasise a lifecycle approach: from research and development, through testing and validation, to deployment and ongoing monitoring.³³ Each phase raises distinct concerns (eg, bias can creep in during training; safety issues may emerge post-deployment), and may involve different responsible parties.³⁴ As an example, in practice, the EU AI Act imposes obligations on providers (*ie*, developers) at the design stage, on deployers (*ie*, users) at the implementation stage, and even envisions post-market monitoring to track the real-world performance of AI systems.

15 An additional dimension to deciding on a definition and scope for AI is about whether to adopt a *technology-specific or technology-agnostic approach*. Notwithstanding the limitations of each approach,³⁵ the broad consensus among governments and experts appears to be that it would be more prudent to adopt technology-neutral and flexible definitions of AI, given concern that overly-specific and technology-based definitions risk becoming obsolete as new AI techniques emerge. An example that demonstrates the challenges of a technology-specific approach lies in the gestation of the EU AI Act when the EU had to double back and account for general-purpose AI systems in the midst of drafting the EU AI Act.³⁶

32 Matt O’Shaughnessy, “One of the Biggest Problems in Regulating AI is Agreeing on a Definition”, *Carnegie Endowment for International Peace Commentary* (6 October 2022) <<https://carnegieendowment.org/posts/2022/10/one-of-the-biggest-problems-in-regulating-ai-is-agreeing-on-a-definition?lang=en>> (accessed 15 December 2025).

33 OECD, *OECD Framework for the Classification of AI Systems* (OECD Digital Economy Papers No 323) (OECD Publishing, 2022) at p 19 <https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/02/oecd-framework-for-the-classification-of-ai-systems_336a8b57/cb6d9eca-en.pdf> (accessed 15 December 2025).

34 OECD, *Scoping the OECD AI Principles: Deliberations of the Expert Group on Artificial Intelligence at the OECD (AIGO)* (OECD Digital Economy Papers No 291) (OECD Publishing, 2019) at p 13 <https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/11/scoping-the-oecd-ai-principles_71e1b6dc/d62f618a-en.pdf> (accessed 15 December 2025).

35 Paul Ohm, “The Argument Against Technology-Neutral Surveillance Laws” (2010) 88 *Texas Law Review* 1685 at 1697–1698.

36 See Oskar J Gstrein, Noman Haleem & Andrej Zwitter, “General-Purpose AI Regulation and the European Union AI Act” (2024) 13(3) *Internet Policy Review* <<https://policyreview.info/articles/analysis/general-purpose-ai-regulation-and-ai-act>> (accessed 15 December 2025). See also Bernhard Nessler & Christiane Wendehorst, *Commission Guidelines on the Application of the Definition of an AI System and the Prohibited AI Practices Established in the AI Act* (European Law Institute, 2024) <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Response_on_the_definition_of_an_AI_System.pdf> (accessed 15 December 2025).

To balance between ensuring that regulatory frameworks are sufficiently malleable to minimise about-turns in the future and preventing such frameworks from being over-inclusive that it includes technologies not initially contemplated, policymakers and regulators should focus definitions and obligations on the core characteristics and impacts of AI, rather than contemporary buzzwords like “machine learning” or “deep learning”.³⁷ Singapore, for one, has advocated a technology-agnostic stance in its Model AI Governance Framework.³⁸ The overall goal is clear: to ensure that governance remains effective as AI evolves without constantly having to rewrite the rulebook.

16 With these fundamentals established, one can then turn to the question of what regulatory approach(es) jurisdictions should adopt towards AI.

C. Considerations about the appropriate regulatory approach

17 Governments globally have adopted a spectrum of regulatory approaches to AI, influenced by their respective national priorities and considerations. While there are multiple ways of analysing these regulatory approaches, one widely observed way is analysing how “light” or “hard” a regulatory approach is.³⁹ At one end of the spectrum are jurisdictions that adopt light-touch, minimal intervention strategies, such as those in the US or Singapore; at the other end lie jurisdictions with comprehensive oversight regimes, such as the EU, which are often backed by AI-focused laws.

18 It is important to recognise, however, that “regulation” is a broad term that encompasses more than just black-letter law.⁴⁰ In

37 European Commission, Annexes to Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM (2021) 206 Final <https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_2&format=PDF> (accessed 15 December 2025).

38 *Model AI Governance Framework* (Personal Data Protection Commission Singapore, 2nd Ed, 2020) at paras 1.1 and 2.15 <<https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf>> (accessed 15 December 2025).

39 Gary E Marchant & Carlos Ignacio Gutierrez, “Soft Law 2.0: An Agile and Effective Governance Approach for Artificial Intelligence” (2023) 24(2) *Minnesota Journal of Law, Science & Technology* <<https://ssrn.com/abstract=4473812>> (accessed 15 December 2025).

40 Julia Black, *Decentred Regulation: Critical Reflections on Regulation* (CARR Discussion Paper No 4) (London School of Economics, 2002) at p 21 <<https://eprints.lse.ac.uk/35985/1/Disspaper4-1.pdf>> (accessed 15 December 2025):
(cont'd on the next page)

practice, AI is governed through a mix of hard law, soft law, and even technical measures. Formal legal rules (statutes, regulations and binding directives) are one pillar – these provide enforceable obligations and penalties for non-compliance. But equally significant are standards and guidelines developed by governments, international bodies, or industry groups which, while not always legally binding, shape best practices. For instance, soft law instruments like ethical AI guidelines, industry codes of conduct, or certification schemes have been proliferated.⁴¹ These may not carry the force of law, but they influence behaviour by setting expectations and norms.⁴² Technical standards (for the purposes of enabling the interoperability of regulatory frameworks, or for safety testing, *etc*) also play a regulatory role by establishing benchmarks for products.⁴³ In the fast-moving tech sector, such non-binding measures can often be implemented faster and updated more easily than formal legislation.⁴⁴ Additionally, market forces and societal pressure (otherwise referred to as “regulation by norms”) guide AI development. Companies may self-regulate by instituting AI ethics boards or conducting audits, in response to public concern or to pre-empt stricter laws.⁴⁵

“Regulation is the sustained and focused attempt to alter the behaviour of others according to defined standards or purposes with the intention of producing a broadly defined outcome or outcomes, which may involve mechanisms of standard-setting, information-gathering and behaviour-modification.”

- 41 See Gary Marchant, “Soft Law’ Governance of Artificial Intelligence”, *AI PULSE* (25 January 2019) at pp 5–11 <<https://perma.cc/5HZD-YKX8>> (accessed 15 December 2025). See also Gary Marchant, Lucille Tournas & Carlos Ignacio Gutierrez, “Emerging Technologies Through Soft Law: Lessons for Artificial Intelligence – An Introduction” (2020) 61 *Jurimetrics: The Journal of Law, Science, and Technology* <<https://lsi.asulaw.org/softlaw/wp-content/uploads/sites/7/2021/04/01-18-gets-through-soft-law-special-issue-intro.pdf>> (accessed 15 December 2025).
- 42 Gary Marchant, Lucille Tournas & Carlos Ignacio Gutierrez, “Emerging Technologies Through Soft Law: Lessons for Artificial Intelligence – An Introduction” (2020) 61 *Jurimetrics: The Journal of Law, Science, and Technology* <<https://lsi.asulaw.org/softlaw/wp-content/uploads/sites/7/2021/04/01-18-gets-through-soft-law-special-issue-intro.pdf>> (accessed 15 December 2025).
- 43 Ana Alania *et al*, *Looking Ahead: The Role of Standards in the Future of Artificial Intelligence (AI) Governance* (University of College London, 2022) <https://www.ucl.ac.uk/steapp/sites/steapp/files/looking_ahead_the_role_of_standards_in_the_future_of_ai_governance_v2.0.pdf> (accessed 15 December 2025).
- 44 Gary Marchant, Lucille Tournas & Carlos Ignacio Gutierrez, “Emerging Technologies Through Soft Law: Lessons for Artificial Intelligence – An Introduction” (2020) 61 *Jurimetrics: The Journal of Law, Science, and Technology* <<https://lsi.asulaw.org/softlaw/wp-content/uploads/sites/7/2021/04/01-18-gets-through-soft-law-special-issue-intro.pdf>> (accessed 15 December 2025).
- 45 Gary Marchant, Lucille Tournas & Carlos Ignacio Gutierrez, “Emerging Technologies Through Soft Law: Lessons for Artificial Intelligence – An Introduction” (2020) 61 *Jurimetrics: The Journal of Law, Science, and Technology* <<https://lsi.asulaw.org/softlaw/wp-content/uploads/sites/7/2021/04/01-18-gets-through-soft-law-special-issue-intro.pdf>> (accessed 15 December 2025).

19 In short, AI governance often operates on multiple levels, with holistic governance of AI requiring a portfolio of tools, combining carrots and sticks. However, notwithstanding the fact that one might see a jurisdiction like the US as a “light-touch” jurisdiction and the EU as taking a “hard” regulatory approach, the fact is that many jurisdictions adopt a “blended” approach and differ only in degree. In the EU, even before the AI Act comes fully into force, the European Commission has been seeking voluntary commitments from AI developers to abide by key principles of the EU AI Act (through an “AI Pact”).⁴⁶ To date, more than 230 companies have signed the EU AI Pact.⁴⁷ On the other hand, a number of US states have already introduced hard AI legislation, including California, Colorado and Texas.

20 It should also be remembered that a jurisdiction’s regulatory approach towards AI often takes reference largely from its economic objectives, risk appetite, and institutional capacity, among other factors. A jurisdiction’s economic objectives and its risk appetite are closely linked, with jurisdictions prioritising AI-driven economic growth leaning toward lighter regulation, out of concern that strict rules could drive away investment or stifle innovation. One such jurisdiction is the US, which sees heavy regulation of AI as a threat to AI innovation⁴⁸ – a view that first emerged in the late 2010s and has recently re-emerged in the US.⁴⁹ This view, also being advanced by major US technology companies,⁵⁰ reflects a higher risk tolerance and willingness to accept risks posed

46 European Commission, “AI Pact” <<https://digital-strategy.ec.europa.eu/en/policies/ai-pact>> (accessed 15 December 2025).

47 See European Commission, “AI Pact” <<https://digital-strategy.ec.europa.eu/en/policies/ai-pact>> (accessed 15 December 2025).

48 Memorandum for the Heads of Executive Departments and Agencies from Office of Management and Budget <<https://bidenwhitehouse.archives.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf>> (accessed 6 January 2026).

49 Ken D Kumayama, Stuart D Levi & William E Ridgway, “US Federal Regulation of AI is Likely to be Lighter, but States May Fill the Void”, *Skadden* (14 January 2025) <<https://www.skadden.com/insights/publications/2025/01/2025-insights-sections/revisiting-regulations-and-policies/us-federal-regulation-of-ai-is-likely-to-be-lighter>> (accessed 15 December 2025). See also Memorandum for the Heads of Executive Departments and Agencies from Office of Management and Budget (3 April 2025) <<https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf>> (accessed 15 December 2025).

50 “Tech Leaders Urge Congress for ‘Light-Touch’ AI Regulations”, *PYMNTS* (8 May 2025) <<https://www.pymnts.com/news/artificial-intelligence/2025/tech-leaders-urge-congress-light-touch-ai-regulations/>> (accessed 15 December 2025). See also US Senate Committee on Commerce, Science & Transportation, “Winning the AI Race: Strengthening U.S. Capabilities in Computing and Innovation” (8 May 2025) <https://www.commerce.senate.gov/2025/5/winning-the-ai-race-strengthening-u-s-capabilities-in-computing-and-innovation_2> (accessed 15 December 2025).

by AI as a trade-off for faster technology development and greater competitiveness. In contrast, the EU, guided by a more precautionary ethos and strong consumer protection values, is showing a lower risk appetite: it is willing to bear the cost of compliance so as to avert harm and build public trust in AI. A jurisdiction's institutional capacity is also a key consideration. For instance, the EU's institutional experience in regulating technologies (as seen with data privacy laws) gave it ballast in enacting an omnibus AI Act.⁵¹ Smaller states or those early in their regulatory development may instead tend towards wait-and-see strategies. For instance, Singapore has positioned itself as a "rule-taker",⁵² preferring to observe international developments and incrementally adjust its domestic regime. However, Singapore goes one step further than merely passively accepting developments, instead adopting a soft governance approach towards AI,⁵³ preferring initiatives such as governance and testing frameworks as well as sandboxes. From the Singapore regulator's perspective, pursuing soft regulation over hard regulation provides more time to learn more about AI technology, better appreciate its benefits and risks, and keep a close eye on how the dynamics of AI governance plays out globally before deciding on which camp to follow; from an industry perspective, companies have some leeway to innovate without being bogged down by regulatory concerns and also some buffer time to put in place new practices that align with the Government's broad principles and non-binding recommendations; and from society's perspective, members of the public can seek recourse from existing laws and regulations. Yet, regardless of differences in regulatory approach, all regulatory approaches must ultimately serve certain core objectives and be designed to withstand the test of time, as the next section discusses.

D. Considerations about governance objectives and regulatory policy design

21 AI governance does not occur in a vacuum. As with any regulatory design, it is shaped by several persistent challenges. One major challenge is information asymmetry. The developers of AI systems typically have far greater knowledge about how these systems work than regulators, users, or affected persons. Peering inside AI systems – including processes around how underlying models are trained, tested and selected – would

51 Vagelis Papakonstantinou & Paul De Hert, "The Regulation of Digital Technologies in the EU: The Law-Making Phenomena of 'Act-ification', 'GDPR Mimesis' and 'EU Law Brutality'" (2020) *Technology and Regulation* 48 <<https://doi.org/10.26116/techreg.2022.005>> (accessed 15 December 2025).

52 Pang Cheng Kit, Kit, "A Comparative Analysis of Artificial Intelligence Regulation: Implications for Singapore" (2025) SAclJ 189 at para 74.

53 Pang Cheng Kit, Kit, "A Comparative Analysis of Artificial Intelligence Regulation: Implications for Singapore" (2025) SAclJ 189 at para 61.

thus be extraordinarily difficult for end-users or regulatory agencies. This asymmetry can leave users uninformed about why an AI system produced a certain decision. Regulators, likewise, may find themselves reliant on the representations of AI companies, lacking independent means to verify their claims. A good governance system must therefore find ways to bridge this gap, whether through transparency requirements, audit powers, or third-party oversight, to ensure that the fox is not always guarding the henhouse.

22 A related challenge is the opacity of many AI systems, which impacts transparency and accountability. Modern AI techniques, particularly deep learning, often work in a manner not intuitively interpretable by humans. As models grow more complex, “the ability of non-specialists to understand how a given output has been reached diminishes”.⁵⁴ This opacity is problematic in a legal context: how can a party be held accountable for an AI-driven decision when even experts cannot readily explain the chain of reasoning? Consequently, one governance priority is to enhance *transparency* where possible – for instance, by imposing obligations for transparency and explainability (which require AI developers or deployers to implement plans to explain the results of AI decision-making, or to grant users the right to receive clear explanations from developers or deployers about the role of AI systems in decisions that significantly impact their health, safety or fundamental rights)⁵⁵ or traceability (ensuring that an AI model’s decisions, and the datasets and processes that yield the AI model’s decisions are documented in an easily understandable way⁵⁶). However, transparency ought not to be absolute:⁵⁷ too much disclosure may risk exposing trade secrets or enable malicious actors to bypass safety measures. Therefore, a reasonable and proportionate governance framework must seek a balance, demanding enough transparency to enable oversight and recourse within an appropriate context, without forcing companies to reveal legitimate trade secrets or details of their proprietary algorithms.

54 Simon Chesterman, “Through a Glass, Darkly: Artificial Intelligence and the Problem of Opacity” (2021) 69(2) *The American Journal of Comparative Law* 271 <<https://doi.org/10.1093/ajcl/avab012>> (accessed 15 December 2025).

55 Future of Privacy Forum, “SK-AI Framework Act Comparison Table” (May 2025) <<https://fpf.org/wp-content/uploads/2025/05/SK-AI-Framework-Act-Comparison-Table.pdf>> (accessed 15 December 2025).

56 *Model AI Governance Framework* (Personal Data Protection Commission Singapore, 2nd Ed, 2020) at para 3.36 <<https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf>> (accessed 15 December 2025).

57 *Model AI Governance Framework* (Personal Data Protection Commission Singapore, 2nd Ed, 2020) at para 3.61 <<https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf>> (accessed 15 December 2025).

23 Given these inherent hurdles, AI governance frameworks must be carefully designed for both *robustness* and *flexibility*. They need to be robust and clear enough to provide legal certainty, allowing stakeholders to know the rules of the road and the standards they are expected to meet. Simultaneously, frameworks must be flexible and adaptive. For example, some jurisdictions include periodic review clauses in their AI strategies or regulatory frameworks, mandating re-evaluation of the rules every few years.⁵⁸ This ensures a built-in opportunity to course-correct as technology advances or circumstances change.

24 Herein, however, lies a “paradoxical challenge” for regulators: they must anticipate future developments of AI while addressing present realities, else they would risk their efforts quickly being rendered irrelevant.⁵⁹ Hence, beyond robustness and flexibility, a further regulatory design goal is *agility*.⁶⁰ This refers to a governance model that can respond to new information and novel applications of AI without lengthy legislative deadlock. Sandboxing approaches (where new AI applications are tested under regulatory supervision) and outcome-based (rather than technology-prescriptive) regulations are examples of policy tools that can be adopted to achieve this agility.⁶¹ Another approach gaining traction among several Asia-Pacific jurisdictions is to confer executive rule-making powers to certain government agencies or committees, so that these bodies may quickly introduce rules and safeguards should the need arise.⁶²

25 Against this backdrop, one can identify several key policy objectives that AI governance frameworks commonly pursue:

58 See, eg, Art 112 of the EU AI Act.

59 Hugo Neuillé, “The Chicken or the Egg’ of AI Regulation”, *Tech Policy Press* (22 January 2025) <<https://www.techpolicy.press/the-chicken-or-the-egg-of-ai-regulation/>> (accessed 16 December 2025).

60 Yeong Zee Kin, *Technology Regulation in the Digital Economy* (Academy Publishing, 2023) at para 2.25.

61 Yeong Zee Kin, *Technology Regulation in the Digital Economy* (Academy Publishing, 2023) at paras 2.45–2.50.

62 See for instance, Japan’s Act on Promotion of Research, Development, and Utilization of Artificial Intelligence-Related Technologies (“AI Promotion Act”) Act No 53 of 2025 and South Korea’s Framework Act on the Development of Artificial Intelligence and Establishment of Trust (“AI Framework Act”) Law No 20676. See Dominic Paulger, “Understanding Japan’s AI Promotion Act: An ‘Innovation-First’ Blueprint for AI Regulation”, *Future of Privacy Forum* (5 July 2025) <<https://fpf.org/blog/understanding-japans-ai-promotion-act-an-innovation-first-blueprint-for-ai-regulation/>> (accessed 16 December 2025) and Sakshi Shivhare & Kwang Bae Park, “South Korea’s New AI Framework Act: A Balancing Act Between Innovation and Regulation”, *Future of Privacy Forum* (18 April 2025) <<https://fpf.org/blog/south-koreas-new-ai-framework-act-a-balancing-act-between-innovation-and-regulation/>> (accessed 16 December 2025).

(a) Firstly, *fostering innovation*. This tends to be a primary objective, as policymakers and regulators are generally keen to maximise the potential of the very technology that promises economic growth and social benefits.

(b) Secondly, *upholding societal rules, principles and values* (or as recognised in certain jurisdictions, fundamental rights). These include privacy laws and rights, addressing (or at least not entrenching) bias and discrimination, especially towards vulnerable or less-privileged groups, and other human rights that automated decision-making might implicate. Doing so is key to ensuring that the output and outcomes of AI systems – and how that output is used – is trustworthy and aligned with societal norms.

(c) Thirdly, ensuring *accountability*. In broad terms, accountability over the outcomes produced by AI systems refers to having a party that can be held responsible and is able to correct the outcome going forward if things were to go wrong. This may entail clear allocation of legal liability (*eg*, producers being liable for defective AI products, or employers being liable for erroneous or biased AI decisions in the workplace) and establishing oversight mechanisms (*eg*, audits or impact assessments) that build accountability into the AI lifecycle.

(d) Fourthly, promoting public *trust* in AI is both an objective and a byproduct of achieving the other goals. Without trust, society will under-utilise genuinely beneficial AI solutions, and paranoia or backlash may set in. Building trust involves transparency, as mentioned, and also participation – giving stakeholders (especially those impacted by AI, such as consumers or employees) a voice in how it is deployed.

(e) Fifthly, modern governance increasingly emphasises *regulatory interoperability* and *international alignment*. As the nature of the lifecycle of AI systems and the impact of their output is inherently borderless, a patchwork of globally incompatible governance frameworks could take jurisdictions further away from the policy objectives covered above. Ensuring regulatory interoperability means that, *eg*, an AI system recognised as meeting the regulatory requirements in one jurisdiction can then be more easily deployed in another, because the regulatory requirements in both jurisdictions have common ground.

(f) Sixthly, policymakers are mindful of *maintaining the competitiveness* of their respective AI ecosystems, above and beyond fostering the act of AI innovation. In a global race for AI supremacy, countries and regions do not want to fall behind

due to onerous regulation. There is a constant search for the sweet spot that safeguards the public and upholds ethical standards, while attracting AI talent and investment. The presence of clear rules can actually enhance competitiveness in the long run (by creating a stable environment for innovation and by fostering public trust which drives adoption), but if overdone, it may drive innovators to less regulated pastures. Hence, competitiveness becomes a litmus test: rules should ideally not disadvantage domestic AI developers *vis-à-vis* international rivals.

26 Balancing these objectives can be challenging, as they sometimes pull in different directions. For example, maximising transparency to ensure accountability could conflict with enhancing competitiveness and innovation. A well-designed governance approach will try to strike a sensible, proportionate, and sustainable equilibrium. In sum, AI governance should be purpose-driven, with a clear-eyed view of the outcomes it seeks (innovation, safeguards, accountability, *etc*), and built to endure the shifts of technological progress.

E. Considerations about implementing regulations and governance policies

27 There is a saying among policymakers that “a policy is only as good as how it is implemented”.⁶³ Translating the considerations above into effective real-world practice is perhaps the most formidable task of all. The following paragraphs cover several key elements that must be considered when considering how best to *implement* an AI governance policy in any particular jurisdiction.

28 A first and fundamental element is technical capacity. Regulators and oversight bodies frequently struggle to keep pace with the rapid advancements in AI technology. The issue comes down to an expertise gap: due to the weight of incentives present in industry and academia, these sectors tend to be where AI specialists are concentrated. This in turn means that government agencies often lack sufficient in-house technical knowledge to appreciate complex AI systems and ecosystems. This challenge is made more daunting by the velocity of AI innovation. By the

63 Eddie Teo, Chairman, Public Service Commission, “Defending Scholarships but not all Scholars”, speech at the 2009 Singapore Seminar in London (31 October 2009) <<https://www.psc.gov.sg/resources/news>> (accessed 16 December 2025). Put in other words, “The best regulatory frameworks are nothing without enforcement.”: see Philipp Hacker, Ramayya Krishnan & Marco Mauer, “Global AI Governance – Part 2: The Power of the Deployer States”, *Oxford Business Law Blog* (10 December 2024) <<https://blogs.law.ox.ac.uk/oblb/blog-post/2024/12/global-ai-governance-part-2-power-deployer-states>> (accessed 16 December 2025).

time a government agency grasps the ins and outs of one AI technology, the field may have already moved on to new architectures and techniques.

29 The second element is resource limitation. Not every government agency has the resources to hire a team of PhD-level data scientists or create dedicated AI units. In smaller jurisdictions especially, regulators wear multiple hats and might oversee AI as only one part of a broader portfolio, limiting the bandwidth they can devote to staying on the cutting edge. Where a jurisdiction does decide to implement harder AI rules, effective monitoring and enforcement may also be constrained by limited resources. Regulatory agencies may not have the manpower, technical capabilities, ability and time to respond to complaints, conduct investigations or audits. In fact, such resource constraints already exist for the enforcement of existing laws (*eg*, data protection laws) due to lack of resources and the sheer number of violations. In the AI context, the situation could be even more acute. If every algorithmic decision were to require auditing, enforcement bodies would predictably be quickly overwhelmed. For this reason, capacity-building must be a key part of regulatory efforts. Policymakers and regulators must undergo training in relevant technical and policy areas, and should be provided the right tools to conduct enforcement work. Without sufficient capacity, even the most well-designed regulatory frameworks may end up as paper tigers.

30 The third element is regulatory co-ordination, both within governments and internationally. As AI's impacts cut across sectoral boundaries, domestic governance often requires multiple agencies to collaborate. For instance, from a regulatory perspective, an AI application used in healthcare may raise data protection issues (overseen by the data regulator), safety issues (overseen by the medical device regulator), and possibly competition issues (overseen by the competition regulator). Siloed oversight could lead to regulatory gaps or inconsistent enforcement. Some jurisdictions have responded by setting up inter-agency task forces on AI or central AI offices to co-ordinate policy. Nevertheless, ensuring smooth collaboration and clear division of responsibility is an ongoing challenge – bureaucratic turf wars, communication breakdowns or differences in resources could impede effective oversight.

31 On the international stage, co-ordination becomes even more complex.⁶⁴ Each country crafting its own AI framework leads

64 In a speech at the IMF Per Jacobsson Foundation Lecture 2025 on 15 October 2025, President of the Republic of Singapore Tharman Shanmugaratnam described the governance of AI as “probably the most complex public policy challenge” faced by the world. See Tharman Shanmugaratnam, President of the Republic of Singapore, “An Era of Possibility: Renewing Economic Order and Shared Purpose”, lecture at the International Monetary Fund in Washington DC (15 October 2025) <<https://www.imf.org/en/News/Articles/2025/10/15/251015-tharman-shanmugaratnam-lecture>> (cont'd on the next page)

to a mosaic of regulations that companies must navigate, potentially slowing innovation and creating opportunities for regulatory arbitrage. Yet, achieving global consensus on AI governance is daunting (to say the least). Nations have differing priorities and interests; *eg*, what one country deems an unacceptable risk (say, a ban on autonomous weapons or predictive policing algorithms) may be actively pursued by another jurisdiction. While there have been positive steps to find common ground – such as in late 2023, when the UK convened an AI Safety Summit at Bletchley Park where 29 countries signed a declaration to work together on safe AI development; or at forums like the G7 (with the Hiroshima AI Process), OECD and the United Nations – translating high-level principles and statements into clear and harmonised action remains challenging. A further dimension is the issue of involving the private sector and civil society internationally. Truly global AI governance will need intricate multi-stakeholder co-ordination across borders, but this is a tall order under present circumstances.

32 The fourth element is meaningful enforcement and compliance. Should a jurisdiction choose to establish hard regulations regulating the development, deployment and adoption of AI (which, it should be stressed, is neither a linear nor necessary step from a soft regulatory approach – although it would usually be hard to reverse), designing and enforcing the regulations in a way that the regulated subjects *understand how to comply* is also a consideration. This is in large part due to the technically opaque nature of AI systems, which makes it challenging for regulators, regulated entities and affected individuals to detect violations. So, for instance, if a law were to impose a substantive (as opposed to procedural or formal) requirement on AI systems such as “non-discrimination” or “accuracy”,⁶⁵ how can one prove that the AI system or application is doing so? It might require access to datasets, system logs, or even the source code – and companies may be reluctant to provide these for proprietary or security reasons. Further, some AI properties (like “fairness” or “accountability”) currently *lack universally agreed metrics*. For instance, the technical community is still debating how best to measure fairness in machine learning amongst multiple competing definitions. Without any consensus amongst the technical community, it follows that regulators would struggle to establish a clear benchmark for compliance with outcome-based regulation. In such situations, outcome-based regulation can be coupled with process-based enforcement mechanisms. For instance, to demonstrate compliance with

istana.gov.sg/Newsroom/Speeches/2025/10/25/An-era-of-possibility-Renewing-economic-order-and-shared-purpose-by-President-Tharman-Shanmugaratnam> (accessed 16 December 2025).

65 This is in fact required, to an extent, under Art 15(1) of the EU AI Act.

a statutory obligation to ensure the safety for all users of their service, AI service providers could be required to conduct an *ex-ante* safety assessment of the AI service in question. The question here is how to ensure that compliance does not become simply a check-box exercise with little impact on real-world outcomes. A further complication is *enforcement jurisdiction*: Given that AI systems can be offered across borders, if an AI system causes harm in Jurisdiction A but was developed in Jurisdiction B and is running on servers in Jurisdiction C, which jurisdiction has enforcement jurisdiction? Existing legal frameworks (like conflict of laws, or e-commerce rules) provide some guidance, but AI's decentralised nature may exploit gaps between jurisdictions. This again circles back to the need for international co-operation: regulators may have to share information or take joint actions for cross-border AI incidents.

33 The fifth element is about keeping the regulatory framework up-to-date, and having in place mechanisms to review and update them as conditions change. This could involve formal sunset clauses that force re-examination of a rule after a set period, or informal but regular consultations with industry and academia to keep abreast of technological shifts. Several jurisdictions have adopted the practice of iterative governance *via* sandboxes or pilot programs – rolling out governance measures in a controlled environment, observing outcomes, and then refining the approach. Additionally, some regulators have been willing to quickly issue supplementary guidance when new AI technologies emerge onto the scene. For instance, as generative AI use became widely ubiquitous, data protection authorities in Singapore, New Zealand, Australia, South Korea, and Japan were relatively quick in issuing guidance on how to comply with data protection laws given these new developments. All these illustrate a need for agility in rule-making and enforcement. In this regard, addressing the dynamics of a fast-changing regulatory environment arguably requires agile regulation and jurisdictions to rapidly iterate through the Observe, Orient, Decide, Act loop to foster a culture of continuous improvement.

34 Having set out some of the most fundamental considerations in AI governance and jurisdictions, the following section examines Singapore's approach to AI governance and regulation.

III. Singapore's approach to artificial intelligence governance and regulation

A. *Background and context*

35 Singapore adopts a broadly innovation-oriented regulatory approach towards AI. Its current high-level policy direction for AI is set out in the Singapore National AI Strategy 2.0 (“NAIS 2.0”), which was launched in 2023 and precedes the first National AI Strategy launched in 2019.⁶⁶ Specifically, the vision is “for Singapore to be a place where AI serves as a force for good, and where we harness AI to uplift and empower our people and businesses”.⁶⁷

36 In working towards its vision, Singapore adopts a “blended approach”, drawing on both hard and soft regulation. For hard regulation, while Singapore does not have an omnibus piece of AI legislation, it relies on existing laws (including the Personal Data Protection Act 2012⁶⁸ and the Copyright Act 2021⁶⁹) and targeted amendments of these laws when necessary to tackle novel issues brought about by AI (including the Elections (Integrity of Online Advertising) (Amendment) Act 2024⁷⁰ (“ELIONA”)). ELIONA targets misinformation in online election advertising caused, for instance, by generative AI through making it an offence for a person to publish manipulated online election advertising containing realistic but false representation of election candidates.⁷¹ For soft regulation, Singapore has released comprehensive guidelines,⁷² guidelines for specific types of AI technology,⁷³ AI governance testing

66 *NAIS 2.0 Singapore National AI Strategy: AI for the Public Good for Singapore and the World* (Ministry of Digital Development and Information, 2023) <<https://file.gov.sg/nais2023.pdf>> (accessed 16 December 2025).

67 *NAIS 2.0 Singapore National AI Strategy: AI for the Public Good for Singapore and the World* (Ministry of Digital Development and Information, 2023) at p 3 <<https://file.gov.sg/nais2023.pdf>> (accessed 16 December 2025).

68 2020 Rev Ed.

69 2020 Rev Ed.

70 Act 34 of 2024.

71 Parliamentary Elections Act 1954 (2020 Rev Ed) s 61MA.

72 *Model AI Governance Framework* (Personal Data Protection Commission Singapore, 2nd Ed, 2020) at paras 1.1 and 2.15 <<https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf>> (accessed 15 December 2025).

73 *Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems* (Personal Data Protection Commission Singapore, 2024) <<https://www.pdpc.gov.sg/guidelines-and-consultation/2024/02/advisory-guidelines-on-use-of-personal-data-in-ai-recommendation-and-decision-systems>> (accessed 16 December 2025).

frameworks and toolkits,⁷⁴ guidelines for specific industry sectors,⁷⁵ and also implemented sandboxes.⁷⁶ The broad mentality behind this blended approach is essentially thus: to introduce hard laws only where there is a pressing and perceptible risk or harm that cannot be adequately addressed by existing legislation; but otherwise, to use softer regulatory tools to incrementally shape responsible behaviour. Only when the target segment of society has largely arrived at a desired baseline level of behaviour (in the form of established industry norms and practices), should regulations or regulators step in to set a baseline floor.⁷⁷

37 On the international plane, while Singapore’s small size invariably constrains its potential as a rule-maker,⁷⁸ Singapore has strategically maintained its position as a global thought leader in AI governance and regulation. The section below will also briefly cover how Singapore has done so.

B. Key features of Singapore’s artificial intelligence governance landscape

38 Following from the broad overview, this section now examines in greater detail three key tenets that underpin Singapore’s AI governance landscape.

39 The first tenet is *non-binding guidelines and governance frameworks*. These efforts began around January 2019, when Singapore’s data protection authority, the Personal Data Protection Commission (“PDPC”), released its first edition of the Model AI Governance Framework (“MGF”).⁷⁹ The MGF is an accountability-based governance framework setting out voluntary recommendations for industry

74 See *AI Verify Testing Framework* (Infocomm Media Development Authority & AI Verify Foundation, 2025) <<https://file.go.gov.sg/aivtf-pdf.pdf>> (accessed 7 January 2026). See also <<https://github.com/aiverify-foundation/aiverify>> and <<https://github.com/aiverify-foundation/moonshot-cicd>>.

75 Monetary Authority of Singapore, “Principles to Promote Fairness, Ethics, Accountability and Transparency (“FEAT”) in the Use of Artificial Intelligence and Data Analytics in Singapore’s Financial Sector” (12 November 2018) <<https://www.mas.gov.sg/publications/monographs-or-information-paper/2018/feat>> (accessed 16 December 2025).

76 The IMDA Generative AI Sandbox which empowers small and medium enterprises to trial generative AI solutions.

77 Yeong Zee Kin, *Technology Regulation in the Digital Economy* (Academy Publishing, 2023) at para 2.38.

78 See para 20, n 52 above.

79 *Model AI Governance Framework* (Personal Data Protection Commission Singapore, 2019) <<https://ai.bsa.org/wp-content/uploads/2019/09/Model-AI-Framework-First-Edition.pdf>> (accessed 16 December 2025).

organisations looking to deploy AI systems at scale. The key contribution of the document lies in applying several key ethical AI principles (namely, fairness, explainability, transparency, safety and human-centricity) to the lifecycle of AI deployment, thus deriving a suite of recommendations that industry players can implement to mitigate AI-associated risks.⁸⁰

40 Apart from the algorithm-agnostic and sector-agnostic MGF, Singapore has released algorithm-specific governance frameworks and guidelines on AI recommendation and decision systems, generative AI, and agentic AI,⁸¹ and sector-specific principles for the financial and healthcare sectors.⁸² Singapore has also released guidelines targeting specific risks, including privacy and cybersecurity risks.⁸³ While these algorithm-specific, sector-specific, and risk-specific governance frameworks and guidelines are useful for supplementing the MGF, the increasing number leaves the industry with a complex web of

-
- 80 Yeong Zee Kin, *Technology Regulation in the Digital Economy* (Academy Publishing, 2023) at para 2.43.
- 81 *Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems* (Personal Data Protection Commission Singapore, 2024) <<https://www.pdpc.gov.sg/guidelines-and-consultation/2024/02/advisory-guidelines-on-use-of-personal-data-in-ai-recommendation-and-decision-systems>> (accessed 16 December 2025); *Model AI Governance Framework for Generative AI: Fostering a Trusted Ecosystem* (AI Verify Foundation & Infocomm Media Development Authority) <<https://aiverifyfoundation.sg/wp-content/uploads/2024/06/Model-AI-Governance-Framework-for-Generative-AI-19-June-2024.pdf>> (accessed 16 December 2025). Singapore also launched a Model AI Governance Framework for Agentic AI on 22 January 2026. See <<https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2026/new-model-ai-governance-framework-for-agentic-ai>> (accessed 26 January 2026).
- 82 Monetary Authority of Singapore, “Principles to Promote Fairness, Ethics, Accountability and Transparency (“FEAT”) in the Use of Artificial Intelligence and Data Analytics in Singapore’s Financial Sector” (12 November 2018) <<https://www.mas.gov.sg/publications/monographs-or-information-paper/2018/feat>> (accessed 16 December 2025); Monetary Authority of Singapore, “Artificial Intelligence Model Risk Management Observations from A Thematic Review” (5 December 2024) <<https://www.mas.gov.sg/-/media/mas-media-library/publications/monographs-or-information-paper/imd/2024/information-paper-on-ai-risk-management-final.pdf>> (accessed 16 December 2024); *Artificial Intelligence in Healthcare Guidelines* (Ministry of Health Singapore *et al*, 2021) <[https://isomer-user-content.by.gov.sg/3/9c0db09d-104c-48af-87c9-17e01695c67c/1-0-artificial-in-healthcare-guidelines-\(aihgle\)_publishedoct21.pdf](https://isomer-user-content.by.gov.sg/3/9c0db09d-104c-48af-87c9-17e01695c67c/1-0-artificial-in-healthcare-guidelines-(aihgle)_publishedoct21.pdf)> (accessed 16 December 2025).
- 83 *Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems* (Personal Data Protection Commission Singapore, 2024) <<https://www.pdpc.gov.sg/guidelines-and-consultation/2024/02/advisory-guidelines-on-use-of-personal-data-in-ai-recommendation-and-decision-systems>> (accessed 16 December 2025); *Guidelines On Securing AI Systems* (Cybersecurity Agency of Singapore, 2024) <<https://isomer-user-content.by.gov.sg/36/e05d8194-91c4-4314-87d4-0c0e013598fc/Guidelines%20on%20Securing%20AI%20Systems.pdf>> (accessed 16 December 2025).

recommendations that they have to navigate. This article proposes the creation of a one-stop summary of how the various guidelines are co-related, for instance, providing references to the relevant guidelines for each type of risk.

41 The second tenet is AI *governance testing*, in line with the race for the development of standards for AI globally. Singapore's key projects are AI Verify and Project Moonshot for traditional AI and generative AI models respectively. AI Verify is an AI governance testing framework and toolkit under which organisations use a combination of technical tests and process-based checks to conduct a voluntary self-assessment of their AI systems.⁸⁴ For instance, where an organisation wishes to test the transparency of its AI model, AI Verify would allow it to conduct a process check of the documents provided to individuals impacted by the AI system to assess whether crucial information (such as the use of AI in the system and the risks involved) is relayed to these individuals.⁸⁵ AI Verify was reported to have been used by companies like IBM and Singapore Airlines during the pilot testing phase,⁸⁶ and the AI Verify testing community has shown encouraging (albeit gradual) signs of growth.⁸⁷ The PDPC has been introducing efforts to increase the take-up rate in the nascent AI governance testing industry, including mapping AI Verify's testing framework to international AI governance frameworks,⁸⁸ and launching the Global AI Assurance Pilot to match testing providers with firms that are deploying generative AI applications.⁸⁹

84 Josh Lee Kok Thong, "AI Verify: Singapore's AI Governance Testing Initiative Explained", *Future of Privacy Forum* (6 June 2023) <<https://fpf.org/blog/ai-verify-singapores-ai-governance-testing-initiative-explained/>> (accessed 16 December 2025).

85 AI Verify, "AI Verify Testing Report" at p 5 <https://aiverifyfoundation.sg/downloads/AI_Verify_Sample_Report.pdf> (accessed 16 December 2025).

86 Sheila Chiang, "Singapore is Not Looking to Regulate A.I. Just Yet, Says the City-State's Authority", *CNBC* (19 June 2023) <<https://www.cnn.com/2023/06/19/singapore-is-not-looking-to-regulate-ai-just-yet-says-the-city-state.html>> (accessed 16 December 2025).

87 Infocomm Media Development Authority, "Building a Trusted, Innovation Ecosystem for AI" (31 May 2024) <<https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/factsheets/2024/project-moonshot>> (accessed 16 December 2025).

88 Infocomm Media Development Authority, "Joint Mapping Exercise Between Singapore IMDA and the US NIST" (10 October 2023) <<https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/nist-irma-joint-mapping-exercise>> (accessed 16 December 2025); AI Verify Foundation, "New Crosswalk with ISO/IEC 42001: 2023 Shows International Alignment" <<https://aiverifyfoundation.sg/resources/#crosswalk-with-iso42001>> (accessed 16 December 2025).

89 AI Verify Foundation, "Global AI Assurance Pilot" <<https://aiverifyfoundation.sg/ai-assurance-pilot/>> (accessed 16 December 2025).

42 Project Moonshot was released into open beta on 31 May 2024 and offers both benchmarking (*ie*, evaluation of a large language model (“LLM”) against industry standards) and red-teaming assessments (*ie*, creation of prompts to attempt to induce misbehaviours in the LLM in order to discover new vulnerabilities).⁹⁰ While it bears similarities to AI Verify as a testing tool, Project Moonshot’s testing capabilities have been tailored specifically to address the risks in LLMs. For one, rather than administering the same generic tests on all LLMs, Project Moonshot offers specialised benchmark tests including for Tamil language and Medical LLMs.⁹¹

43 The third tenet is *regulatory sandboxes*, which are programmes that industry players can apply for in order to “obtain a waiver from specific legal provisions or compliance processes to allow them to innovate.”⁹² In contrast to traditional policy tools which tend to stifle innovation, regulatory sandboxes instead complement Singapore’s pro-innovation landscape, supporting innovation in regulated sectors by creating space for piloting these technologies.⁹³ Regulatory sandboxes are not new to Singapore, which has previously established both licensing and statutory regulatory sandboxes for other purposes such as autonomous vehicles and FinTech products (which may involve the use of AI).⁹⁴ In relation to AI, Singapore has established three regulatory sandboxes. The first is a GenAI Sandbox to promote the adoption of generative AI solutions by small and medium-sized enterprises (“SMEs”).⁹⁵ The other two

90 Infocomm Media Development Authority, “Project Moonshot, Powered by AI Verify, and AI Collaborations” (31 May 2024) <<https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/factsheets/2024/project-moonshot>> (accessed 16 December 2025).

91 Tan Tee Jim SC *et al*, “IMDA and AI Verify Foundation Finalise Governance Framework for Generative AI and Launch Project Moonshot”, *Legal Update: Lee & Lee* at p 3 <<https://www.leenlee.com.sg/news-publications/2024/07/imda-and-ai-verify-foundation-finalise-governance-framework-for-generative-ai-and-launch-project-moonshot>> citing AI Verify Foundation Moonshot Dataset <<https://github.com/aiverify-foundation/moonshot-data>> (accessed 16 December 2025).

92 OECD, *Regulatory Sandboxes in Artificial Intelligence* (OECD Digital Economy Papers No 356) (OECD Publishing, 2023) at p 8 <https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/07/regulatory-sandboxes-in-artificial-intelligence_a44aae4f/8f80a0e6-en.pdf> (accessed 16 December 2025).

93 *Law and Technology in Singapore* (Simon Chesterman, Goh Yihan & Andrew Phang Boon Leong eds) (Academy Publishing, 2021) at para 4.101.

94 Road Traffic (Autonomous Motor Vehicles) Rules 2017; Monetary Authority of Singapore, “Overview of Regulatory Sandbox” <<https://www.mas.gov.sg/development/fintech/regulatory-sandbox>> (accessed 16 December 2025).

95 Infocomm Media Development Authority, “Building on the Success of Singapore’s First Generative AI Sandbox for SMEs, IMDA Launches Generative AI Sandbox for SMEs v2.0 to Help SMEs Adopt GenAI Solutions” (29 October 2024) <<https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/factsheets/2024/gen-ai-sandbox-2-0>> (accessed 16 December 2025).

sandboxes build on Singapore’s AI testing and development framework: the Generative AI Evaluation Sandbox seeks to develop common benchmarks and tests for LLM evaluations,⁹⁶ and the Global AI Assurance Sandbox is a platform through which developers and deployers globally can have their GenAI applications tested by specialist technical testers.⁹⁷

44 The synergy between these three tenets has been crucial for fostering trust in AI, ensuring that Singapore remains competitive in the AI domain not just in the short-term, but also in the long run.

C. *Singapore’s footprint in the global AI landscape through international collaboration and efforts*

45 Having discussed Singapore’s domestic AI governance efforts, this article now examines Singapore’s efforts on a global plane. To put things in context, international collaboration is a key pillar of Singapore’s approach to AI governance, as is crystallised in Singapore’s first National AI Strategy,⁹⁸ and further reiterated in the NAIS 2.0 as an intent to establish Singapore as “an ambitious and pragmatic international partner on AI innovation and governance”.⁹⁹ This pillar has been reinforced in several ways. Firstly, Singapore actively engages in *bilateral efforts* with other jurisdictions through crosswalks, trade agreements, and Memorandums of Understanding.¹⁰⁰ One example is the crosswalk between the US National Institute of Standards and Technology’s (“NIST”) AI Risk Management Framework (“NIST AI RMF”) and Singapore’s Infocomm Media Development Authority’s (“IMDA”) AI Verify. The crosswalk allows users whose AI systems have satisfied certain criteria under AI Verify to state that they would have satisfied the

96 Infocomm Media Development Authority, “First of its Kind Generative AI Evaluation Sandbox for Trusted AI by AI Verify Foundation and IMDA” (31 October 2024) <<https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/generative-ai-evaluation-sandbox>> (accessed 16 December 2025).

97 Infocomm Media Development Authority, “Global AI Assurance Sandbox” at p 2 <<https://file.go.gov.sg/aivf-sandbox-overview.pdf>> (accessed 16 December 2025).

98 *National Artificial Intelligence Strategy: Advancing our Smart Nation Journey* (Smart Nation & Digital Government Office, 2019) <<https://file.go.gov.sg/nais2019.pdf>> (accessed 16 December 2025).

99 *NAIS 2.0 Singapore National AI Strategy: AI for the Public Good for Singapore and the World* (Ministry of Digital Development and Information, 2023) <<https://file.go.gov.sg/nais2023.pdf>> (accessed 16 December 2025).

100 Artificial intelligence governance also features in multiple trade agreements and Memorandums of Understanding Singapore has signed with multiple jurisdictions, including the US, EU, UK, South Korea, ASEAN, and more. See Jones E, Kira B & Tavengerwei R “Norm Entrepreneurship in Digital Trade: The Singapore-led Wave of Digital Trade Agreements” (2024) 23(2) *World Trade Review* 208 at 224.

equivalent criteria under the NIST AI RMF, and *vice versa*.¹⁰¹ As alluded to earlier, such bilateral efforts are small but vital steps towards building demand for Singapore's AI governance efforts and its AI industry.

46 Secondly, Singapore is gradually establishing its position as a *facilitator of inter-jurisdictional conversations* around AI governance, both regionally and internationally. For one, Singapore serves as the convenor of the Digital Forum of Small States ("FOSS"), bringing digital policy leaders from small states together to exchange views on pressing digital challenges.¹⁰² AI Singapore also serves as the co-chair of the Working Group on Innovation & Commercialization of the Global Partnership on Artificial Intelligence, which brings together 42 experts and 11 specialists from around the globe to conduct research projects.¹⁰³ Ongoing projects include research for the broad adoption of AI by SMEs and to protect AI innovation and intellectual property.¹⁰⁴ Beyond multinational fora, Singapore has taken steps to co-operate with other jurisdictions bilaterally and multilaterally. For example, provisions on co-operating on AI governance increasingly feature in bilateral trade agreements and digital economy agreements.¹⁰⁵

47 Thirdly, Singapore *contributes to the global AI governance literature* by publishing guidelines, frameworks, and reports with widespread applicability. In September 2024, the Digital FOSS

101 Josh Lee Kok Thong, "Explaining the Crosswalk Between Singapore's AI Verify Testing Framework and The U.S. NIST AI Risk Management Framework", *Future of Privacy Forum* (23 January 2024) <<https://fpf.org/blog/explaining-the-crosswalk-between-singapores-ai-verify-testing-framework-and-the-u-s-nist-ai-risk-management-framework/>> (accessed 16 December 2025). See also the actual Crosswalk document <<https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/nist-imda-joint-mapping-exercise>> and an updated Crosswalk for generative AI <<https://file.go.gov.sg/crosswalk-aivtfxairmf-genaiprofile.pdf>>.

102 *AI Playbook for Small States* (Infocomm Media Development Authority & Rwanda Ministry of ICT and Innovation, 2024) at p 11 <<https://www.imda.gov.sg/-/media/imda/files/news-and-events/media-room/media-releases/2024/09/ai-playbook-for-small-states/imda-ai-playbook-for-small-states.pdf>> (accessed 16 December 2025).

103 The Global Partnership on Artificial Intelligence, *Innovation and Commercialization Working Group Report* (November 2022) at p 5 <<https://wp.oecd.ai/app/uploads/2025/05/gpai-innovation-commercialization-wg-report-2022.pdf>> (accessed 7 January 2026).

104 See <<https://oecd.ai/en/working-group-innovation-and-commercialisation/>> (accessed 7 January 2026).

105 See, for instance, Infocomm Media Development Authority, "Media Factsheet: Digital Economy Agreements" (3 March 2020) <<https://www.imda.gov.sg/-/media/imda/files/about/media-releases/2020/cos2020/annex-h-cos-2020---factsheet---digital-economy-agreements.pdf>> (accessed 16 December 2025) and "World's First AI Trade Provision in Korea-Singapore Deal?", *APAC GATES* (15 December 2023) <<https://apacgates.com/insights/f/worlds-first-ai-trade-provision-in-korea-singapore-deal>> (accessed 16 December 2025).

launched the AI Playbook for Small States, which outlines key issues and considerations for policymakers in the development, use and governance of AI, from the perspective of small states.¹⁰⁶ This initiative allows Singapore to contribute towards capacity building, while building ease-of-recall (also known in bureaucratic speak as “mindshare”) in Singapore as a leader in AI governance. In February 2025, Singapore’s IMDA published the “Singapore AI Safety Red Teaming Challenge Evaluation Report 2025”, which establishes a methodology to test LLMs for context-specific concerns in different languages and cultures.¹⁰⁷ In May 2025, following from the 2025 Singapore Conference on AI: International Scientific Exchange on AI Safety, a report titled “The Singapore Consensus on Global AI Safety Research Priorities” was published. The report synthesises and identifies research priorities in technical AI safety, facilitating global conversations and international research collaboration.¹⁰⁸

48 All in all, Singapore’s domestic and global efforts work in tandem to ensure that Singapore remains contextually relevant. With that, the following section examines how other jurisdictions have tackled the question of AI governance, and also identifies the commonalities and divergences between these approaches. Rather than focusing on the specific obligations imposed on industry players, the following section will explore the general approach and the policy tools utilised by each jurisdiction.

106 *AI Playbook for Small States* (Infocomm Media Development Authority & Rwanda Ministry of ICT and Innovation, 2024) <<https://www.imda.gov.sg/-/media/imda/files/news-and-events/media-room/media-releases/2024/09/ai-playbook-for-small-states/imda-ai-playbook-for-small-states.pdf>> (accessed 16 December 2025).

107 Infocomm Media Development Authority, “Singapore AI Safety Red Teaming Challenge Evaluation Report” (February 2025) <<https://www.imda.gov.sg/-/media/imda/files/about/emerging-tech-and-research/artificial-intelligence/singapore-ai-safety-red-teaming-challenge-evaluation-report.pdf>> (accessed 16 December 2025).

108 Singapore Conference on AI & Infocomm Media Development Authority, “The Singapore Consensus on Global AI Safety Research Priorities: Building a Trustworthy, Reliable and Secure AI Ecosystem” (8 May 2025) at p 5 <<https://file.go.gov.sg/sg-consensus-ai-safety.pdf>> (accessed 16 December 2025); Singapore Conference on AI, “The Singapore Consensus on Global AI Safety Research Priorities” (8 May 2025) <<https://www.scai.gov.sg/2025/scai2025-report/>> (accessed 16 December 2025).

IV. Global efforts in artificial intelligence regulation

A. *On a jurisdictional plane*

(1) *United States*

(a) Background and context

49 In the US, the high-level policy direction has been in a state of flux due to the changes in administration. The direction for the Trump administration is set out in “America’s AI Action Plan” (which was released on 10 July 2025)¹⁰⁹ following from an Executive Order issued in January 2025, which effectively replaced the Biden administration’s Executive Order on the Safe, Secure and Trustworthy Development and Use of Artificial Intelligence. Broadly, the Trump administration encourages pro-growth AI policies and the deregulation of AI as “AI is far too important to smother in bureaucracy at this early stage”.¹¹⁰ These deregulatory efforts will begin with the identification of (amongst others) existing federal regulations, administrative orders, guidance documents and prior Federal Trade Commission investigations which hinder AI innovation and adoption.¹¹¹ This outlook will undoubtedly affect state-level regulations, with the Action Plan providing that “[t]he Federal government should not allow AI-related Federal funding to be directed toward states with burdensome AI regulations that waste these funds”.¹¹² The Trump Administration also specifically highlights three pillars, namely accelerate AI innovation, build American AI infrastructure, and lead in international AI diplomacy and security.¹¹³

109 The White House, “Winning the Race: America’s AI Action Plan” (July 2025) <<https://whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>> (accessed 16 December 2025).

110 The White House, “Winning the Race: America’s AI Action Plan” (July 2025) at p 3 <<https://whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>> (accessed 16 December 2025); Caitlin Andrews, “The Outlook for AI Safety Regulation in the US”, *IAPP* (12 February 2025) <[https://iapp.org/news/a/the-outlook-for-ai-safety-in-the-u-s->](https://iapp.org/news/a/the-outlook-for-ai-safety-in-the-u-s-) (accessed 17 December 2025); Joe Duball, “Deregulation, Competition Take Center Stage at AI Action Summit”, *IAPP* (11 February 2025) <<https://iapp.org/news/a/deregulation-competition-take-center-stage-at-ai-action-summit>> (accessed 17 December 2025).

111 The White House, “Winning the Race: America’s AI Action Plan” (July 2025) at p 3 <<https://whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>> (accessed 17 December 2025).

112 The White House, “Winning the Race: America’s AI Action Plan” (July 2025) at p 3 <<https://whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>> (accessed 17 December 2025).

113 The White House, “Winning the Race: America’s AI Action Plan” (July 2025) at p 1 <<https://whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>> (accessed 17 December 2025).

(b) Broad overview of federal and state-level AI governance

50 The US's AI regulatory landscape comprises federal and state-level regulation relating to AI, while also relying on existing laws. Unfortunately, with federal agencies and states being given free rein to regulate (in so far as it is within their mandates), this has resulted in a fragmented AI regulatory landscape not only within each level, but also between the federal and state levels.

51 At the federal level, the US draws on a range of regulatory tools. On one end of the spectrum, several federal laws relating to AI have been enacted by the US Congress, including the National Artificial Intelligence Initiative Act of 2020 which established the National Artificial Intelligence Initiative Office and co-ordinated AI research and development efforts. On 19 May 2025, President Trump signed the TAKE IT DOWN Act into law, which prohibits the online publication of intimate visual depictions of non-consenting adults and minors (including deepfakes) and requires named platforms to establish processes to notify such individuals and to accommodate requests for removal of such depictions.¹¹⁴ No omnibus legislation regulating AI has been enacted, in line with how – as some academics have noted – the US appears to favour a vertical regulatory approach.¹¹⁵ Thus far, federal agencies have been releasing guidance documents and clarifying the application of existing laws in view of the specific risks that arise in their respective sectors.¹¹⁶ For instance, the US Consumer Financial Protection Bureau released a circular clarifying that federal consumer financial laws apply regardless of the technology being used, even if the technology is too complicated or opaque to understand.¹¹⁷

52 On the other end of the spectrum, the US has also relied on, and is expected to increasingly rely on, soft regulatory tools. For one, the

114 Senate Bill 146: TAKE IT DOWN Act (119th Congress (2025–2026) <<https://www.congress.gov/bill/119th-congress/senate-bill/146/text>> (accessed 17 December 2025).

115 Davtyan T, “The US approach to AI Regulation: Federal Laws, Policies, and Strategies Explained”, 16(2) *Journal of Law, Technology, & the Internet* 223 at 227.

116 Davtyan T, “The US approach to AI Regulation: Federal Laws, Policies, and Strategies Explained”, 16(2) *Journal of Law, Technology, & the Internet* 223 at 229, citing Federal Trade Commission *et al*, “Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems”, press release (25 April 2023) <https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf> (accessed 17 December 2025).

117 Consumer Financial Protection Bureau, “Consumer Financial Protection Circular 2022-03” (26 May 2022) <<https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/>> (accessed 17 December 2025).

Biden-Harris administration had secured voluntary commitments from a number of leading AI companies (including Google and Salesforce) to help advance the development of safe, secure, and trustworthy AI.¹¹⁸ After a year, in 2024, the voluntary commitments saw some success as these companies actively adjusted their development processes to align with the principles of responsible AI development.¹¹⁹ However, the future of these voluntary commitments is uncertain since the January 2025 Executive Order had expressly revoked the Biden administration's AI policies.

53 As regards state-level AI governance, numerous pieces of AI-related legislation have been enacted, with states like California and Colorado being more active in the AI regulation scene than others. However, this has resulted in a patchwork of state regulation, which businesses have to navigate in order to operate across state lines.¹²⁰ Although it would be ideal for this regulatory fragmentation to be resolved by federal standardisation,¹²¹ this is unlikely due to the Trump administration's general reluctance to regulate or introduce guardrails on AI.

54 Notably, the Colorado AI Act¹²² ("CAIA") was the first omnibus state-level AI regulation to be passed in the US in May 2024. The CAIA is slated to come into effect on 30 June 2026. The CAIA (as it stands) adopts a risk-based approach, similar to the EU AI Act, focusing on

118 The White House, "Fact Sheet: Biden-Harris Administration Secures Voluntary Commitments from Eight Additional Artificial Intelligence Companies to Manage the Risks Posed by AI", press release <<https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/09/12/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-eight-additional-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/>> (accessed 17 December 2025).

119 Melissa Heikkilä, "AI Companies Promised to Self-Regulate One Year Ago. What's Changed?", *MIT Technology Review* (22 July 2024) <<https://www.technologyreview.com/2024/07/22/1095193/ai-companies-promised-the-white-house-to-self-regulate-one-year-ago-whats-changed/>> (accessed 17 December 2025).

120 Justine Gluck, Beth Do & Tatiana Rice, "The State of State AI: Legislative Approaches to AI in 2025", *Future of Privacy Forum* (October 2025) <<https://fpf.org/wp-content/uploads/2025/10/The-State-of-State-AI-2025.pdf>> (accessed 17 December 2025); Gregory S Dawson *et al*, "How different states are approaching AI", *Brookings* (18 August 2025) <<https://www.brookings.edu/articles/how-different-states-are-approaching-ai/>> (accessed 17 December 2025).

121 Simon J Evenett, Johannes Fritz & Tommaso Giardini, "Tough on the Outside, Soft on the Inside: The Likely Evolution of AI Governance under Trump", *I by IMD* (17 January 2025) <<https://www.imd.org/ibyimd/artificial-intelligence/tough-on-the-outside-soft-on-the-inside-the-likely-evolution-of-ai-governance-under-trump/>> (accessed 17 December 2025).

122 Senate Bill 24-205: Consumer Protections for Artificial Intelligence (2024) (Colorado AI Act) ("CAIA") <<https://leg.colorado.gov/bills/sb25b-004>> (accessed 17 December 2025).

consumer protection and algorithmic discrimination.¹²³ The CAIA specifically targets high-risk AI systems, which are AI systems that make consequential decisions with “a material legal or similarly significant effect on” areas including education, employment, and financial or lending services.¹²⁴ The CAIA imposes transparency and accountability obligations, as well as a duty to avoid algorithmic discrimination on AI developers and deployers of high-risk AI systems. One interesting feature is how the CAIA facilitates interoperability with other regimes, for instance, by expressly providing that impact assessments conducted in compliance with other laws would also meet the CAIA’s requirements.¹²⁵

55 Rather than running through more pieces of state-level AI legislation, this article focuses on providing a broad overview of state-level AI legislation, highlighting four points in this respect. Firstly, state-level AI legislation has been gradually introduced in a measured manner, whether it be in relation to specific use cases or types of AI technologies. In relation to use cases, state-level AI legislation that has been enacted largely pertain to AI systems used in consequential decisions that materially impact individuals, such as AI systems which impact education or essential government services.¹²⁶ In relation to technology-specific approaches, states have enacted AI legislation or advanced bills regulating technologies including chatbots, frontier/foundation models and generative AI.¹²⁷ Secondly, the obligations that are

123 Jariwala M, “A Comparative Analysis of the EU AI Act and the Colorado AI Act: Regulatory Approaches to Artificial Intelligence Governance” (2024) 186(28) *International Journal of Computer Applications* 23.

124 CAIA ss 1(3) and 1(9)(a).

125 CAIA ss 6-1-1703(3)(e). See Tatiana Rice, Keir Lamont & Jordan Francis, “The Colorado Artificial Intelligence Act” (FPF U.S. State AI Legislation Report), *Future of Privacy Forum* (July 2024) at p 12 <https://fpf.org/wp-content/uploads/2024/07/FPF-Legislation-Policy-Brief_-The-Colorado-AI-Act-Final.pdf> (accessed 18 December 2025).

126 Tatiana Rice, Jordan Francis & Keir Lamont, “U.S. State AI Legislation: How U.S. State Policymakers are Approaching Artificial Intelligence Regulation” (FPF U.S. Legislation Report), *Future of Privacy Forum* (September 2024) at pp 4–5 <<https://fpf.org/wp-content/uploads/2024/09/FINAL-State-AI-Legislation-Report-webpage.pdf>> (accessed 18 December 2025); Justine Gluck, Beth Do & Tatiana Rice, “The State of State AI: Legislative Approaches to AI in 2025”, *Future of Privacy Forum* (October 2025) at p 6 <<https://fpf.org/wp-content/uploads/2025/10/The-State-of-State-AI-2025.pdf>> (accessed 18 December 2025); Gregory S Dawson *et al*, “How different states are approaching AI”, *Brookings* (18 August 2025) <<https://www.brookings.edu/articles/how-different-states-are-approaching-ai/>> (accessed 18 December 2025).

127 Justine Gluck, Beth Do & Tatiana Rice, “The State of State AI: Legislative Approaches to AI in 2025”, *Future of Privacy Forum* (October 2025) at pp 9–12 <<https://fpf.org/wp-content/uploads/2025/10/The-State-of-State-AI-2025.pdf>> (accessed 18 December 2025); Richard Sentinella & Cobun Zweifel-Keegan, “US State AI Legislation: Reviewing the 2025 Session”, *IAPP* (16 July 2025) <<https://iapp.org/>> (cont’d on the next page)

commonly imposed on developers and deployers include transparency and disclosure obligations, obligations mandating that risk/impact assessments and audits be carried out, and also requiring organisations to develop AI governance programmes which meet certain criteria (eg, requiring a certain number of persons to be responsible for overseeing the programme).¹²⁸ Thirdly, rights which have been granted to consumers in multiple pieces of state-level legislation include the right to notice and explanation about the use of an AI system, the right to correct inaccurate information used in decision-making, and the right to appeal or opt-out of an automated decision.¹²⁹ Fourthly, in the majority of proposals and pieces of state legislation, enforcement is carried out by the respective state's Attorney General's office.¹³⁰

(c) Other notable initiatives

56 Apart from the soft regulatory tools mentioned above, there are three other non-traditional regulatory efforts which the authors wish to draw attention to. Two of these initiatives are by the US NIST, which is part of the US Department of Commerce and has been actively conducting research and developing measurements, evaluations, standards and guidelines for AI. The first initiative is the NIST AI RMF, which is a voluntary guide for organisations and individuals to frame and address the risks of AI systems in practice.¹³¹ In hopes of facilitating conformance, the NIST has established crosswalks by mapping concepts and terms between the AI RMF and other frameworks including Singapore's AI Verify, Japan's AI Guidelines for Business, and Korea's Guidebook for Development of Trustworthy AI.¹³² However, it remains to be seen how the NIST AI RMF and its crosswalks will be revised

news/a/us-state-ai-legislation-reviewing-the-2025-session> (accessed 18 December 2025).

128 Tatiana Rice, Jordan Francis & Keir Lamont, "U.S. State AI Legislation: How U.S. State Policymakers are Approaching Artificial Intelligence Regulation", *Future of Privacy Forum* (September 2024) at pp 12–13 <<https://fpf.org/wp-content/uploads/2024/09/FINAL-State-AI-Legislation-Report-webpage.pdf>> (accessed 18 December 2025).

129 Tatiana Rice, Jordan Francis & Keir Lamont, "U.S. State AI Legislation: How U.S. State Policymakers are Approaching Artificial Intelligence Regulation", *Future of Privacy Forum* (September 2024) at p 14 <<https://fpf.org/wp-content/uploads/2024/09/FINAL-State-AI-Legislation-Report-webpage.pdf>> (accessed 18 December 2025).

130 Tatiana Rice, Jordan Francis & Keir Lamont, "U.S. State AI Legislation: How U.S. State Policymakers are Approaching Artificial Intelligence Regulation", *Future of Privacy Forum* (September 2024) at p 16 <<https://fpf.org/wp-content/uploads/2024/09/FINAL-State-AI-Legislation-Report-webpage.pdf>> (accessed 18 December 2025).

131 National Institute of Standards and Technology, "AI Risk Management Framework" <<https://www.nist.gov/itl/ai-risk-management-framework>> (accessed 18 December 2025).

132 National Institute of Standards and Technology, "Crosswalk Documents" <<https://airc.nist.gov/airmf-resources/crosswalks/>> (accessed 18 December 2025).

following recommendations under America's AI Action Plan to "eliminate references to misinformation, Diversity, Equity, and Inclusion, and climate change".¹³³ The other initiative is NIST's Assessing Risks and Impacts of AI ("ARIA") program, which confirms an AI system's claimed capabilities, understands how risks arise, and investigates the potential positive and negative impacts of the model under regular use.¹³⁴ More such programmes will likely be launched following recommendations under America's AI Action Plan to "accelerate the development and adoption of national standards for AI systems".¹³⁵ With jurisdiction like the US and Singapore developing their own AI testing programmes/frameworks, other jurisdictions may follow in suit. This would open up potential for greater inter-jurisdictional collaboration and interoperability.

57 The final initiative is the implementation of *regulatory sandboxes*. The US has not established any regulatory sandboxes for AI at a federal level as of yet, although these will likely soon be in the works following recommendations in America's AI Action Plan for the implementation of regulatory sandboxes "where researchers, startups, and established enterprises can rapidly deploy and test AI tools while committing to open sharing of data and results".¹³⁶ Regulatory sandboxes have already been proposed at the state-level, with one such proposal being a bipartisan Bill introduced by US senator Mike Rounds before the US Congress titled "Unleashing AI Innovation in Financial Services Act". Under s 2(7) of the Bill, regulated financial entities would be able to test AI test projects without the fear of enforcement actions looming over their heads.¹³⁷ This bill has been referred to the Committee on Banking, Housing and Urban Affairs.¹³⁸ Regulatory sandboxes also feature in the high-profile Texas Responsible AI Governance Act ("TRAIGA"), which was passed by the Texas Legislature on 2 June 2025. Under Chapter 552, AI systems can

133 The White House, "Winning the Race: America's AI Action Plan" (July 2025) at p 4 <<https://whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>> (accessed 18 December 2025).

134 National Institute of Standards and Technology, "The NIST Assessing Risks and Impacts of AI (ARIA) Pilot Evaluation Plan" (2024) at p 11 <https://ai-challenges.nist.gov/aria/docs/evaluation_plan.pdf> (accessed 18 December 2025).

135 The White House, "Winning the Race: America's AI Action Plan" (July 2025) at p 5 <<https://whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>> (accessed 18 December 2025).

136 The White House, "Winning the Race: America's AI Action Plan" (July 2025) at p 5 <<https://whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>> (accessed 18 December 2025).

137 Senate Bill 2528: Unleashing AI Innovation in Financial Services Act (119th Congress 2025–2026) <https://www.heinrich.senate.gov/imo/media/doc/unleashing_ai_innovation_in_financial_services_act.pdf> (accessed 18 December 2025).

138 Senate Bill 4951: Unleashing AI Innovation in Financial Services Act (118th Congress 2023–2024) <<https://www.congress.gov/bill/118th-congress/senate-bill/4951>> (accessed 18 December 2025).

be tested under its sandbox program for up to 36 months, while being exempted from statutory obligations.¹³⁹

58 To recapitulate, there is considerable complexity in the US's AI regulatory picture, with its canvas woven from the threads of the various initiatives of the federal government and the states. Broadly speaking, the US's landscape can be characterised by its protective stance towards both its domestic AI policies and products, amidst heightening geopolitical pressures. This protectiveness was demonstrated in the US's slew of chip export restrictions and its response to DeepSeek's release of its R1 model on the US app stores by the US Navy, Members of Congress, and state lawmakers alike.¹⁴⁰ In April 2025, the US House Select Committee on the Chinese Communist Party also published a report setting out how "DeepSeek represents a profound threat to [the] nation's security".¹⁴¹ This protective stance may result in the US withholding its support for future global AI governance efforts – a position which would pose a considerable challenge for global harmonisation efforts moving forward in the absence of a major player in the AI industry.

(2) *European Union*

(a) Background and context

59 In the EU, the high-level policy direction for AI is set out in the European Parliament's Digital Transformation Strategy, the European Commission's Digital Decade Policy Programme 2030, and the Coordinated Plan on AI. The EU AI's regulatory landscape comprises pieces of legislation that were already existing (eg, General Data Protection Regulation ("GDPR")) and others which were recently enacted (eg, Digital Services Act, Digital Markets Act, EU AI Act). Notably, the proposed AI Liability Directive has since been withdrawn, as was announced by the European Commission in their 2025 Work Programme. The reasons for this were the co-legislators' (ie, the Council of Member States and the Parliament) inability to reach an agreement and the obsolescence of the

139 Texas Responsible Artificial Intelligence Governance Act (HB 1709) <<https://capitol.texas.gov/tlodocs/89R/billtext/pdf/HB01709L.pdf>> (accessed 18 December 2025).

140 Robert Huffman *et al*, "January 2025 AI Developments – Transitioning to the Trump Administration", *Covington* (12 February 2025) <<https://www.insideglobaltech.com/2025/02/12/january-2025-ai-developments-transitioning-to-the-trump-administration/>> (accessed 18 December 2025).

141 USHouse Select Committee on the Chinese Communist Party, "Deepseek Unmasked: Exposing the CCP's Latest Tool for Spying, Stealing, and Subverting U.S. Export Control Restrictions" (16 April 2025) at p 1 <<https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/DeepSeek%20Final.pdf>> (accessed 18 December 2025).

proposal.¹⁴² This is likely due to the revision of the EU's Product Liability Directive to include software like AI systems. The Directive came into force on 8 December 2024.¹⁴³

60 The EU is considered a global rule-maker, although the extent to which it will be able to shape the global AI governance landscape remains in question. In particular, there is scepticism over whether the same, large-scale “Brussels effect” that occurred with the GDPR would arise for the EU AI Act¹⁴⁴ – *ie*, a promulgation of the Act, or at least aspects of its substantive structure and standards, on a global scale, largely owing to the size and strength of the EU market.¹⁴⁵ This scepticism is amplified in light of the US clearly favouring deregulation, with the US Vice President JD Vance expressly mentioning the US's disagreement with the EU's AI regulatory regime at the 2025 AI Summit,¹⁴⁶ and the US government's Mission to the EU sending a letter to the European Commission expressing its disagreement with numerous aspects of the EU's draft Code of Practice on General-Purpose AI (including the Code's level of prescriptiveness).¹⁴⁷ This will likely result in regulators of other jurisdictions becoming more hesitant in, if not deciding against, regulating. On 19 November 2025, the European Commission published the Digital Omnibus Regulation Proposal (“Digital Omnibus”) which proposes the simplification of rules for several pieces of EU digital legislation.¹⁴⁸ For the EU AI Act, the Digital Omnibus proposes, *inter alia*, delayed implementation timelines, reduced compliance obligations

142 European Commission, “Commission Work Programme 2025” <https://commission.europa.eu/strategy-and-policy/strategy-documents/commission-work-programme/commission-work-programme-2025_en> (accessed 18 December 2025).

143 Maureen Daly & Lynsey Burke, “Revised EU Product Liability Regime Expands to AI Software Providers”, *Pinsent Masons* (20 December 2024) <<https://www.pinsentmasons.com/out-law/analysis/revised-eu-product-liability-regime-expands-ai-software-providers>> (accessed 18 December 2025).

144 Tarafder A & Vadlamani A, “Will the EU AI Regulations Give Rise to Another ‘Brussels Effect’? Lessons from the GDPR” (2025) 10(1) *Journal of Development Policy and Practice* 45 at 53–54; Pagallo U, “Why the AI Act Won't Trigger a Brussels Effect” (2023) *AI Approaches to the Complexity of Legal Systems* (Forthcoming).

145 Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press, 2019) at p 25.

146 JD Vance, Vice President of the US, speech by the Vice President at the Artificial Intelligence Action Summit in Paris, France (11 February 2025) <<https://www.presidency.ucsb.edu/documents/remarks-the-vice-president-the-artificial-intelligence-action-summit-paris-france>> (accessed 18 December 2025).

147 Luca Bertuzzi, “How the US Government Wants to Rewrite EU's Code of Practice for AI Models”, *MLex* (29 April 2025) <<https://www.mlex.com/mlex/articles/2331619/how-the-us-government-wants-to-rewrite-eu-s-code-of-practice-for-ai-models>> (accessed 18 December 2025).

148 European Commission, “Digital Package” <<https://digital-strategy.ec.europa.eu/en/faqs/digital-package>> (accessed 18 December 2025).

for the EU AI Act, and introduces an AI regulatory sandbox at the EU level. There are still chapters to be written on this recent momentum towards deregulation in Europe.

(b) EU AI Act

61 The authors first begin with explaining where the EU AI Act is at in terms of its implementation timeline. The EU AI Act entered into force on 1 August 2024, with the intention being for the Act to fully commence application on 2 August 2026. Transitional periods of differing lengths are applicable based on the obligation and the type of AI system in question: Chapter II on “prohibited AI practices” came into force on 2 February 2025;¹⁴⁹ a transitional period of 12 months was stipulated for obligations on providers of general-purpose AI models (*ie*, such obligations came into force on 2 August 2025) “[g]iven the rapid pace of technological advancements and adoption of general-purpose AI models”.¹⁵⁰ In mid-2025, there was some uncertainty regarding whether the European Commission may postpone enforcement efforts on the provisions which had yet to come into force, with unofficial reports published suggesting delays whereas a spokesperson for the European Commission confirmed that there would be no delay to the EU AI Act’s implementation timeline.¹⁵¹ Potential reasons for such delay included industry and international pressure and delays in the release of guides and code of practices which were meant to accompany the AI Act.¹⁵² Most recently, under the Digital Omnibus, the European Commission has proposed additional transitional periods for some compliance obligations, including obligations for high-risk AI systems and labelling obligations for AI-generated content.¹⁵³

149 EU AI Act Art 113(a).

150 EU AI Act Recital 179.

151 European Commission, “Midday Press Briefing from 04/07/2025” [Video] <<https://audiovisual.ec.europa.eu/en/video/I-274901>> (accessed 18 December 2025); Caitlin Andrews, “European Commission Holds Firm on AI Act Implementation Timeline”, *IAPP* (7 July 2025) <<https://iapp.org/news/a/european-commission-holds-firm-on-ai-act-implementation-timeline>> (accessed 18 December 2025).

152 Danny Tobey *et al*, “The European Commission Considers Pause on AI Act’s Entry into Application”, *DLA Piper* (4 June 2025) <<https://www.dlapiper.com/en/insights/publications/ai-outlook/2025/the-european-commission-considers-pause-on-ai-act-entry-into-application>> (accessed 18 December 2025).

153 European Commission, “Staff Working Document Accompanying Proposal” (19 November 2025) at p 73 <<https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal>> (accessed 18 December 2025); European Commission, “FAQs: Digital Package” <<https://digital-strategy.ec.europa.eu/en/faqs/digital-package>> (accessed 8 January 2026).

62 Next, turning to the Act itself. On a broad level, the EU AI Act adopts a risk-based approach, comprising elements of risk assessment and categorisation, impact assessment and risk management. The EU AI Act also seeks to protect fundamental rights by drawing on the EU founding treaties.¹⁵⁴ However, the EU’s attempt to protect fundamental rights with a risk-based approach has faced criticism. For one, some critic that the EU AI Act’s “technocratic, risk-based approach undermines fundamental human rights by treating them as mere safety concerns, prioritizing market interests over human rights, and reducing AI systems to consumer products.”¹⁵⁵ Others critic that the two concepts are incompatible as risk is assessed at the societal level, while human rights violations are typically against individuals.¹⁵⁶

63 As for the scope of the EU AI Act, the definition of AI is aligned with the OECD’s definition, in hopes of setting precedent for a global definition to reduce legal uncertainty. Even then, the definition in Art 3(1) has been critiqued for being overly broad as it encompasses a wide range of systems – from simple to complex; from machine learning to logic-based systems.

64 The EU AI Act serves as the overarching Act setting out the obligations imposed on providers, deployers, importers, distributors and product manufacturers of AI systems used in the EU. To ensure compliance with the Act, Member States are required to designate or establish a market surveillance authority, a notifying authority, and a national public authority.¹⁵⁷ Member States are then given the discretion to set out the procedure for monitoring and assessing compliance.¹⁵⁸

65 Finally, this article highlights three regulatory tools that have been statutorily encoded in the EU AI Act. The first regulatory tool is the implementation of *regulatory sandboxes*. Under Art 57 of the Act, Member States are required to establish at least one AI regulatory sandbox at the national level, which shall be operational by 2 August 2026. In November

154 Martin Ebers, “Truly Risk-Based Regulation of Artificial Intelligence – How to Implement the EU’s AI Act (19 June 2024) at pp 8 and 11 <<http://dx.doi.org/10.2139/ssrn.4870387>> (accessed 18 December 2025).

155 Oleksandr Svitych, “Blind Transparency: A Critical Discourse Analysis of the EU AI Act” (2025) *Critical Policy Studies* 1 at 3.

156 Martin Ebers, “Truly Risk-Based Regulation of Artificial Intelligence – How to Implement the EU’s AI Act (19 June 2024) at pp 11–12 <<http://dx.doi.org/10.2139/ssrn.4870387>> (accessed 18 December 2025); Marco Almada & Nicolas Petit, *The EU AI Act: A Medley of Product Safety and Fundamental Rights?* (EUI RSC Working Paper, 2023/59) at pp 17–18 <<https://hdl.handle.net/1814/75982>> (accessed 18 December 2025).

157 EU AI Act Recital 153, Arts 77(1) and 77(2).

158 EU AI Act Arts 3(19) and 28.

2023, Spain legislated the first AI regulatory sandbox in accordance with the EU AI Act pursuant to Spanish Royal Decree 817/2023.¹⁵⁹ Under the Digital Omnibus, the EU Commission has proposed establishing an AI regulatory sandbox at the EU level so as to leverage infrastructures across member states and to facilitate cross-border collaboration.¹⁶⁰ The second regulatory tool is the development of *harmonised standards* by the European standardisation organisations, led by the European Committee for Standardization and the European Committee for Electrotechnical Standardization. These standards will be used to assess compliance with the Act. These standards are expected to cover ten concrete aspects of AI, including risk management, transparency, and accuracy.¹⁶¹ The third regulatory tool is the *Code of Practice* under Art 56 of the Act, which general-purpose AI model providers can sign to demonstrate their commitment to comply with obligations in the period before the official standards come into force.¹⁶² Non-signatories would be expected to report their compliance measures to the AI office and may be subject to more requests for information and model evaluations.¹⁶³ The Code of Practice, and its accompanying non-binding guidelines which will clarify how the obligations are to be interpreted and applied, was originally to be published in May or June 2025.¹⁶⁴ It was eventually published on 10 July 2025 and endorsed by the European Commission and the European AI Board on 1 August 2025.¹⁶⁵

66 The upshot here is that the EU's legislative initiatives continue to hold undeniable sway over regulatory thinking globally. Regardless of

159 Paloma Bru, "Spain Legislates for First EU AI Act Regulatory Sandbox", *Pinsent Masons* (13 November 2023) <<https://www.pinsentmasons.com/out-law/news/spain-legislates-for-first-eu-ai-act-regulatory-sandbox>> (accessed 18 December 2025); Spain, Ministry of Economic Affairs and Digital Transformation, Royal Decree 817/2023 <<https://www.boe.es/boe/dias/2023/11/09/pdfs/BOE-A-2023-22767.pdf>> (accessed 18 December 2025).

160 European Commission, "Staff Working Document Accompanying the Proposal" at p 75 <<https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal>> (accessed 18 December 2025).

161 Josep Soler Garrido *et al*, "Harmonised Standards for the European AI Act" (European Commission JRC139430) (24 October 2024) <<https://publications.jrc.ec.europa.eu/repository/handle/JRC139430>> (accessed 18 December 2025).

162 See Arts 53(4) and 55(2) of the EU AI Act.

163 European Commission, "General-Purpose AI Guidelines Consultation" (22 April 2025) at p 17 <<https://digital-strategy.ec.europa.eu/en/news/commission-seeks-input-clarify-rules-general-purpose-ai-models>> (accessed 18 December 2025).

164 European Commission, "General-Purpose AI Guidelines Consultation" (22 April 2025) at pp 1–2 <<https://digital-strategy.ec.europa.eu/en/news/commission-seeks-input-clarify-rules-general-purpose-ai-models>> (accessed 18 December 2025).

165 European Commission, "Drawing-up a General-Purpose AI Code of Practice" <<https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice>> (accessed 13 January 2026).

the result of the present momentum for deregulation, the EU's AI-related laws (including, but not limited to, the EU AI Act) are regulatory realities that companies developing or deploying AI products and services globally ignore at their own peril. After all, even jurisdictions far from the EU – Vietnam¹⁶⁶ and Colorado,¹⁶⁷ for instance – have drafted AI laws containing parallels to core features of the EU AI Act. That said, it appears that fears that the EU had been regulating AI too quickly and aggressively now seem to be catching up to the EU. The EU continues to hold pertinent lessons for Singapore's AI governance journey.

(3) *China*

(a) Background and context

67 In China, the high-level policy direction for AI is set out in the New Generation Artificial Intelligence Development Plan, which was published in 2017.¹⁶⁸ China's AI regulatory landscape comprises both soft and hard regulation. Soft regulatory tools which have been employed include national policies and industrial standards,¹⁶⁹ while hard regulatory tools include existing nationwide laws, administrative regulations and local regulations. Thus far, China has relied on enacting various pieces of hard regulation which target different subsets of AI technology, including algorithm recommendation algorithms, deep synthesis technology, and generative AI. Although a horizontal draft AI law was published by an expert group in March 2024, experts are of the view that horizontal regulation is unlikely in the near future due to considerable disagreement

166 Ministry of Science & Technology, "Draft Law on Artificial Intelligence" (29 September 2025) <<https://mst.gov.vn/van-ban-phap-luat/du-thao/2294.htm>> (accessed 18 December 2025). See also Huu-Tuan Nguyen & Alex Do, "Vietnam's Draft AI Law: Racing Toward Regulation with EU Inspirations", *IAPP* (15 October 2025) <<https://iapp.org/news/a/vietnam-s-draft-ai-law-racing-toward-regulation-with-eu-inspirations>> (accessed 18 December 2025).

167 Senate Bill 24-205: Consumer Protections for Artificial Intelligence (2024) (Colorado AI Act) ("CAIA") <<https://leg.colorado.gov/bills/sb24-205>> (accessed 18 December 2025).

168 The State Council of the People's Republic of China, "Notice: New Generation Artificial Intelligence Development Plan" (8 July 2017) <https://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm> (accessed 18 December 2025); see translated version by Graham Webster *et al*, "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)", *DigiChina* (1 August 2017) <<https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/>> (accessed 30 November 2025).

169 See, eg, T/CESA 1197-2022.

between industry and academics, as well as how AI technology continues to evolve rapidly.¹⁷⁰

(b) China's artificial intelligence regulatory landscape

68 The cornerstone of China's AI regulatory landscape lies in its three pieces of administrative regulations which set out the key obligations for developing and deploying AI systems in China – the Algorithm Recommendation Regulation, the Provisions on Management of Deep Synthesis in Internet Information Service, and the Interim Measures on Management of Generative Artificial Intelligence Services (“Generative AI Measures”). Each piece of hard regulation was developed when there was widespread societal concern regarding the risks of the respective types of AI systems. For instance, the Algorithm Recommendation Regulation was prompted by concerns about how ByteDance was able to dictate user feeds through the use of their recommendation algorithms, and the Generative AI Measures was prompted by the release of ChatGPT.¹⁷¹ Owing to its unique political system, China is able to enact new regulation to fill in the gaps which arise (*ie*, agile regulatory approach).¹⁷²

69 Apart from nationwide AI regulation, China also has *local* AI regulations, although these largely focus on industry development. In particular, some of these local AI regulations statutorily encode the establishment of “pilot zones”, which are similar to regulatory sandboxes under the EU AI Act. Cities deemed by the Chinese government to possess a wealth of scientific education resources, strong industry presence, robust infrastructure, and clear support by the local government towards AI, are designated as “national new generation AI innovation and development pilot zones”.¹⁷³ The local governments of these pilot zones are to facilitate

170 Sylvie Zhuang, “China Likely to Ditch Unified AI Legislation Due to ‘Considerable Disagreement’, Timing”, *South China Morning Post* (17 July 2024) <<https://www.scmp.com/news/china/politics/article/3270544/china-likely-ditch-unified-ai-legislation-due-considerable-disagreement-timing>> (accessed 18 December 2025).

171 Matt Sheehan, “Tracing the Roots of China's AI Regulations”, *Carnegie Endowment for International Peace* (27 February 2024) <<https://carnegieendowment.org/2024/02/27/tracing-roots-of-china-s-ai-regulations-pub-91815>> (accessed 21 April 2025).

172 Pang Cheng Kit, Kit, “A Comparative Analysis of Artificial Intelligence Regulation: Implications for Singapore” (2025) 37 SAclJ 189 at para 44, citing Xiao Baiyang, “Agile and Iterative Governance: China's Regulatory Response to AI” (2024) at pp 8 and 21 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4705898> (accessed 3 January 2026).

173 Guidelines for National New Generation Artificial Intelligence Innovation and Development Pilot Zone Construction Work Section III <https://www.most.gov.cn/xxgk/xinxifenlei/fdzdgnr/fgzc/gfxwj/gfxwj2020/202012/t20201224_171987.html> (accessed 8 January 2026); see version translated by Centre for Security and Emerging Technology at <<https://cset.georgetown.edu/publication/guidelines-for->

(cont'd on the next page)

the testing of AI technology applications and policy tools, the organising of AI-based social experiments and the construction of AI infrastructure by providing a buffer zone.¹⁷⁴ As of 2023, China had established a total of 18 pilot zones.¹⁷⁵ These include the pilot trials in the Regulations for the Promotion of the Development of the Artificial Intelligence Industry in Shanghai Municipality (“Shanghai AI Regulation”) which stipulates a risk-based framework governing the experimentation of AI products,¹⁷⁶ and the Measures of Beijing Municipality on Promoting the Innovative Development of Artificial General Intelligence (“Beijing AGI Regulation”) which “creates a pilot demonstration zone for foundational data systems”.¹⁷⁷ However, these regulations do not appear to provide further details about the pilot trials, such as the criteria for eligibility and the regulatory relief that companies would be entitled to.¹⁷⁸

70 As for soft regulatory tools, in September 2024, the National Technical Committee 260 on Cybersecurity of Standardization Administration of China released the Artificial Intelligence Safety Governance Framework 1.0 (“AI Safety Framework”).¹⁷⁹ The Framework

national-new-generation-artificial-intelligence-innovation-and-development-pilot-zone-construction-work/> (accessed 18 December 2025); and Baiyang Xiao, “Agile and Iterative Governance: China’s Regulatory Response to AI” (25 August 2025) at pp 25–26 <<http://dx.doi.org/10.2139/ssrn.4705898>> (accessed 18 December 2025); “17 AI pilot zones built in China: Official”, *The State Council Information Office, The People’s Republic of China* (7 December 2021) <http://english.scio.gov.cn/chinavoices/2021-12/07/content_77915232.htm> (accessed 18 December 2025).

174 Guidelines for National New Generation Artificial Intelligence Innovation and Development Pilot Zone Construction Work, Section II.

175 “China to Push AI-Enabled Economic, Social Development”, *Global Times* (19 May 2023) <<https://www.globaltimes.cn/page/202305/1290995.shtml>> (accessed 18 December 2025).

176 Regulations for the Promotion of the Development of the Artificial Intelligence Industry in Shanghai Municipality Art 65 <<https://perma.cc/PQ8J-ARCA>>; see version translated by Centre for Security and Emerging Technology at <<https://cset.georgetown.edu/publication/regulations-for-the-promotion-of-the-development-of-the-artificial-intelligence-industry-in-shanghai-municipality/>> (accessed 18 December 2025). See also Baiyang Xiao “Agile and Iterative Governance: China’s Regulatory Response to AI (25 August 2025) at pp 25–26 <<http://dx.doi.org/10.2139/ssrn.4705898>> (accessed 18 December 2025).

177 Regulations for the Promotion of the Development of the Artificial Intelligence Industry in Shanghai Municipality Art 5 <https://www.beijing.gov.cn/zhengce/zhengcefagui/202305/t20230530_3116869.html> (accessed 18 December 2025). See version translated by the People’s Government of Beijing Municipality at <https://english.beijing.gov.cn/investinginbeijing/WhyBeijing/lawpolicy/policies/202307/t20230724_3205629.html> (accessed 18 December 2025).

178 Baiyang Xiao, “Agile and Iterative Governance: China’s Regulatory Response to AI” (25 August 2025) at p 26 <<http://dx.doi.org/10.2139/ssrn.4705898>> (accessed 18 December 2025).

179 “China Unveils AI Safety Governance Framework to Lead Global Standards”, *Geopolitechs* (9 September 2024) <<https://www.geopolitechs.org/p/china-unveils->

(cont’d on the next page)

outlines principles for AI safety governance, classifies AI safety risks, identifies technological measures to address those risks, and provides governance measures and safety guidelines for AI development and application.¹⁸⁰ The AI Safety Framework has since been updated in September 2025 to provide more detailed technical recommendations on governance measures.¹⁸¹

(c) China as a growing convenor of AI discussions

71 Having explored the local Chinese AI regulatory efforts, this subsection examines how China contributes to the global AI landscape. Since 2017, the Chinese State Council has declared that China will actively participate in the global governance of AI,¹⁸² and it has continuously reiterated this collaborative stance.¹⁸³ In October 2023, China had introduced its Global AI Governance Initiative, emphasising the need for a people-centred and ethical approach in the development of AI, while also highlighting the need for international co-operation involving developing countries.¹⁸⁴ In line with these statements, Chinese representatives have been in attendance at every AI safety summit thus

groundbreaking-ai-safety> (accessed 18 December 2025).

- 180 National Technical Committee 260 on Cybersecurity, Standardization Administration of China, “AI Safety Governance Framework (V1.0)” (9 September 2024) <<https://www.tc260.org.cn/upload/2024-09-09/1725849192841090989.pdf>> (accessed 18 December 2025); Danny Tobey *et al*, “China Releases AI Safety Governance Framework”, *DLA Piper* (12 September 2024) <<https://www.dlapiper.com/en-sg/insights/publications/2024/09/china-releases-ai-safety-governance-framework>> (accessed 18 December 2025).
- 181 Cyberspace Administration of China, “Version 2.0 of the Artificial Intelligence Security Governance Framework was Released” (15 September 2025) <https://www.cac.gov.cn/2025-09/15/c_1759653448369123.htm> (accessed 18 December 2025). See also “China Releases Upgraded AI Safety Governance Framework to Tackle Emerging AI Risks”, *Geopolitechs* (16 September 2025) <<https://www.geopolitechs.org/p/china-releases-upgraded-ai-safety>> (accessed 18 December 2025).
- 182 Caroline Meinhardt & Graham Webster, “What Do We Know About China’s New AI Safety Institute?”, *DigiChina* (6 February 2025) <<https://digichina.stanford.edu/work/what-do-we-know-about-chinas-new-ai-safety-institute/>> (accessed 18 December 2025).
- 183 Ministry of Foreign Affairs, People’s Republic of China, “Promoting Development for All and Bridging the AI Divide”, (30 September 2024) <https://www.mfa.gov.cn/eng/wjbzhd/202412/t20241218_11497479.html> (accessed 19 December 2025); Ministry of Foreign Affairs, People’s Republic of China, “Wang Yi on Global AI Governance: Ensure that AI is a Force for Good, Ensure Safety and Ensure Fairness” (7 March 2024) <https://www.mfa.gov.cn/eng/wjbzhd/202403/t20240308_11256430.html> (accessed 19 December 2025).
- 184 Global AI Governance Initiative <<http://no.china-embassy.gov.cn/eng/lcbit/lcwj/202401/P020240112008151194499.pdf>> (accessed 19 December 2025).

far.¹⁸⁵ Apart from contributing as a participant, the relatively new China AI Safety and Development Association, which will represent China in dialogue and collaboration with AI security research institutions around the world, also organised its first event in February 2025.¹⁸⁶

(4) *Commonalities in regulatory philosophies and practices*

(a) Overarching governance frameworks

72 Out of the jurisdictions that were surveyed, Singapore, the US and China each have their respective AI governance frameworks. These provide the first port of call to which organisations and individuals can turn to in order to address the risks of their AI systems. Generally, there is considerable overlap in the principles and risks identified. However, the specific details, how each principle is defined, and the precise recommendations may differ. For instance, both Singapore's MGF and the US's NIST AI RMF highlight the principle of explainability. However, the list of recommendations differs – the NIST AI RMF recommends including a description of the AI system's function tailored to the user's role, knowledge, and skill level;¹⁸⁷ the MGF recommends including descriptions, as well as documenting the model training and selection processes and the use of supplementary explanation tools.¹⁸⁸ Considering the wealth of knowledge lying in these various frameworks, there is much value in establishing crosswalks between a greater number of nations to consolidate such knowledge and to improve interoperability.

(b) Trend towards special rules for certain subsets of AI technologies

73 Each of the jurisdictions surveyed has turned to technology-specific measures on at least one occasion, for instance, publishing guidelines/provisions/regulations specifically relating to generative AI. While this detracts from the technology-neutral

185 Caroline Meinhardt & Graham Webster, "What Do We Know About China's New AI Safety Institute?", *DigiChina* (6 February 2025) <<https://digichina.stanford.edu/work/what-do-we-know-about-chinas-new-ai-safety-instit>>(accessed 18 December 2025).

186 Official website of China AI Safety and Development <<https://cnaisi.cn/sy#>> (accessed 19 December 2025).

187 National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework* (AI RMF 1.0) at pp 16–17 <<https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>> (accessed 19 December 2025).

188 *Model AI Governance Framework* (Personal Data Protection Commission Singapore, 2nd Ed, 2020) at pp 44–45 <<https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf>> (accessed 19 December 2025).

approach adopted by most jurisdictions, such an approach is effective as a stop-gap measure to address new technology that brings about widespread societal concern. However, each jurisdiction ought to exercise prudence in turning to technology-specific measures due to the risk of a fragmented regulatory landscape from the enactment of such further measures. In this regard, a relevant consideration would be the degree of *agility* afforded by the measure in question. A sensible approach when implementing technology-specific measures could be to ensure that the measure can be easily adjusted or revoked to address forthcoming changes in the regulatory environment (such as future technological disruption). For instance, it may still be prudent to introduce voluntary guidance or interim rules on generative AI, as these can be easily “sunset-ed”. On the contrary, hard-coding into legislation obligations tied to fixed benchmarks of computing power could make it challenging to amend should such benchmarks become obsolete in the future. Each jurisdiction must also consider its institutional capacity and the speed at which it is able to implement changes to the regulatory landscape, as this would affect the efficacy of technology-specific measures.

(c) Regulatory sandboxes

74 Regulatory sandboxes have, at the very least, been *considered* in all the jurisdictions surveyed. However, the regulatory sandboxes vary in terms of the sectors which they cover and the leniency of their requirements. Notwithstanding the benefits it offers in facilitating market entry and adapting regulatory processes,¹⁸⁹ regulatory sandboxes are not without challenges. For one, sandboxes are conceived and designed as small-scale testing frameworks with limited cohorts of participants. Regulators may face difficulties with implementing and maintaining the sandboxes should there be excessive demand.¹⁹⁰ Another potential issue is the risk of AI companies forum shopping for the sandbox with the most favourable conditions, which may in turn lead to a race to the

189 OECD, *Regulatory Sandboxes in Artificial Intelligence* (OECD Digital Economy Papers No 356) (OECD Publishing, 2023) at pp 16–17 <https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/07/regulatory-sandboxes-in-artificial-intelligence_a44aae4f/8f80a0e6-en.pdf> (accessed 19 December 2025); Beth Do & Stacey Gray, “Balancing Innovation and Oversight: Regulatory Sandboxes as a Tool for AI Governance”, *Future of Privacy Forum* (4 August 2025) <<https://fpf.org/blog/balancing-innovation-and-oversight-regulatory-sandboxes-as-a-tool-for-ai-governance/>> (accessed 19 December 2025).

190 OECD, *Regulatory Sandboxes in Artificial Intelligence* (OECD Digital Economy Papers No 356) (OECD Publishing, 2023) at p 18 <https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/07/regulatory-sandboxes-in-artificial-intelligence_a44aae4f/8f80a0e6-en.pdf> (accessed 19 December 2025).

bottom between regulators that lower safeguards and requirements to attract innovators.¹⁹¹

75 A further challenge may lie in selecting and attracting the right parties to participate in the sandbox, and relatedly, to ensure that learnings from the sandbox are relevant to the industry at large. Failing to do so could, at the very least, cause the sandbox to lose meaning; at the worst, it could hurt the credibility of the regulator and possibly invite criticism of regulatory capture or bias.

(5) *Divergences in regulatory philosophies and practices*

76 Each jurisdiction's decisions on *when*, *what* and *how* to regulate AI are shaped by a myriad of factors including domestic policy considerations, position in the global AI governance landscape (eg, rule-taker or rule-setter), competitive edge in the AI industry (eg, developer or deployer), geopolitical considerations, and its risk appetite (among other factors).¹⁹²

77 While there is general consensus regarding the risks brought about by AI, the specific risks that each jurisdiction focuses on addressing may differ. For instance, the core principles that Singapore focuses on are explainability, transparency, and fairness – all of which go towards “underwrit[ing] confidence in Singapore’s AI landscape” and “demonstrat[ing] to AI developers that Singapore is a conducive place for responsible AI development” to attract greater interest in Singapore’s AI industry.¹⁹³ This is in contrast to China, which already has a booming AI industry, such that it can turn its resources towards focusing on AI safety governance more generally, which includes inherent technical flaws as well as misuse, abuse, and malicious use of AI.¹⁹⁴

78 The jurisdictions surveyed also adopted a diverse range of policy tools, turning to a mix of both hard and soft regulation. The extent of discretion accorded to *subnational* governments differs between

191 OECD, *Regulatory Sandboxes in Artificial Intelligence* (OECD Digital Economy Papers No 356) (OECD Publishing, 2023) at p 18 <https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/07/regulatory-sandboxes-in-artificial-intelligence_a44aae4f/8f80a0e6-en.pdf> (accessed 19 December 2025).

192 See para 20 above.

193 NAIS 2.0 *Singapore National AI Strategy: AI for the Public Good for Singapore and the World* (Ministry of Digital Development and Information, 2023) at pp 50 and 54 <<https://file.go.gov.sg/nais2023.pdf>> (accessed 19 December 2025).

194 National Technical Committee 260 on Cybersecurity, Standardization Administration of China, “AI Safety Governance Framework (V1.0)” (9 September 2024) at pp 4–5 <<https://www.tc260.org.cn/upload/2024-09-09/1725849192841090989.pdf>> (accessed 19 December 2025).

jurisdictions – while state governments in the US have substantial autonomy from the federal government in deciding how and what to regulate about AI, Chinese local governments have only enacted regulations relating to industry development, and none relating to substantive obligations. Member States in the EU also have little discretion regarding the substantive obligations, with their discretion lying instead in the domain of enforcement. By enacting an overarching national regulation which sets out the substantive obligations, a jurisdiction would be able to guard against fragmentation between national and subnational AI regulation, streamlining compliance obligations for the industry players.

V. Global efforts in regulation

79 The borderless nature of AI development and deployment limits the ability of a purely national regulatory approach to fully address its impact and risks. Thus, notwithstanding the regulatory approaches of the jurisdictions covered above, there is thus a growing recognition that effective AI governance requires co-ordinated international efforts. Notably, the adoption of the OECD's Recommendation of the Council on Artificial Intelligence in May 2019 marked the first time governments came together around a common set of principles for the responsible stewardship of AI.¹⁹⁵ These initial principles-based efforts set the foundation for subsequent discussions, even though they stopped short of creating enforceable international law.

80 In the past few years, AI *governance initiatives* have proliferated across multilateral, regional, and bilateral platforms. Multilateral organisations are actively addressing AI. These include the UN,¹⁹⁶ the

195 Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449, OECD Legal Instruments) (adopted 22 May 2019) <<https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449#mainText>> (accessed 19 December 2025). The Recommendation is now recognised by 48 national governments, as well as the European Union: see <<https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449#adherents>> (accessed 19 December 2025).

196 United Nations, Office for Digital and Emerging Technologies, “High-Level Advisory Body on Artificial Intelligence” <<https://www.un.org/digital-emerging-technologies/ai-advisory-body>> (accessed 19 December 2025).

OECD,¹⁹⁷ the Global Partnership on AI,¹⁹⁸ the Council of Europe,¹⁹⁹ and the Association of Southeast Asian Nations.²⁰⁰ Countries are also strengthening bilateral co-operation through a web of agreements and partnerships focused on AI. The result is a dense network of initiatives spanning all levels of governance.

81 Across these efforts, a set of common priority areas for AI governance has begun to emerge. Policymakers broadly agree on the need to develop technical standards and benchmarks to evaluate AI systems' safety, to address governance challenges posed by "frontier AI" models, and to embark on joint research on AI safety. Another priority is capacity-building – ensuring that all countries (including those with fewer resources or expertise) can implement AI oversight and fully benefit from AI's innovations.²⁰¹

82 Meaningful global regulation of AI, however, faces several formidable challenges. *Geopolitical tensions and divergent national interests* often impede consensus on global rules. For example, when the US and around 60 other countries endorsed new guidelines for the military use of AI, China notably did not support the initiative. Major AI powers also espouse *differing regulatory strategies*, which makes harmonisation of AI regulatory regimes difficult. Another challenge is the *uneven regulatory capacity* across nations: many developing countries do not yet possess the specialised expertise and resources to govern AI effectively, raising concerns about an emerging global "AI divide". Finally, AI's *technical complexity and rapid evolution* make it a moving target for regulators. All of these factors – political tensions, capacity gaps, and the sheer dynamism of the technology – make the implementation of a cohesive global AI governance regime a herculean (albeit worthy) task.

197 Adam Murray, "The OECD Network of Experts on AI: Moving From Principle to Practice for Trustworthy AI", *OECD.AI Policy Observatory* (8 June 2020) <<https://oecd.ai/en/wonk/oecd-network-ai-experts-cooperation-for-trustworthy-beneficial-ai>> (accessed 19 December 2025).

198 OECD, "Global Partnership on Artificial Intelligence" <<https://www.oecd.org/en/about/programmes/global-partnership-on-artificial-intelligence.html>> (accessed 19 December 2025).

199 Council of Europe, "The Framework Convention on Artificial Intelligence" <<https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>> (accessed 19 December 2025).

200 ASEAN, *ASEAN Guide on AI Governance and Ethics* <https://asean.org/wp-content/uploads/2024/02/ASEAN-Guide-on-AI-Governance-and-Ethics_beautified_201223_v2.pdf> (accessed 19 December 2025).

201 For instance, the G7's Hiroshima AI framework devotes a pillar to project-based co-operation in developing tools and best practices for responsible AI.

83 In light of these challenges, the international community is exploring new directions to strengthen AI governance globally. One proposal is to establish dedicated *international monitoring and early-warning systems for advanced AI developments*. The UN High-Level Advisory Body on Artificial Intelligence, for instance, has endorsed the idea of creating an AI watchdog agency inspired by the International Atomic Energy Agency to monitor cutting-edge AI projects worldwide and even verify that leading AI developers are complying with agreed safety measures. There are also calls for improved cross-border communication about AI incidents and vulnerabilities, so that issues identified in one jurisdiction can be rapidly shared and addressed in others. Work is also underway to develop common metrics for evaluating AI systems and to require more transparent reporting of AI models' capabilities and limitations, ensuring that all stakeholders work from a shared reference point. While these efforts are to be lauded, whether they will help build a more coherent and anticipatory global AI governance framework remains to be seen.

VI. Takeaways and concluding observations for Singapore

84 With the foregoing analysis, this final section distils key lessons and offers forward-looking recommendations. It weaves together considerations around Singapore's unique context, opportunities for regulatory development, addressing the issue of timing in introducing new regulatory frameworks, and Singapore's approach towards the international AI governance landscape.

A. *Singapore's context and strategic considerations*

85 Singapore's own position as a small, open, highly interconnected city-state, as well as its status as "deployer state", are immutable truths that shape its regulatory strategy. These unchanging parameters set constraints that help focus the context for AI regulatory debates in Singapore. Paradoxically, rather than limiting Singapore's AI potential, it has catalysed a largely coherent and centrally co-ordinated policy approach that helps Singapore avoid intra-jurisdiction fragmentation or mis-coordination sometimes seen in larger jurisdictions. A further advantage to Singapore's compactness is its compact governance structure – along with close co-ordination among policy and regulatory agencies – that allows it to implement AI initiatives with operational efficiency and consistency. These three advantages – *clarity* (relative to other jurisdictions) in regulatory objectives; strong internal *co-ordination*;

and *coherence* in implementation – have allowed Singapore to master “masterly inactivity”²⁰² (in response to the challenge of timing regulation).

86 Singapore’s enduring realities, however, also present unique challenges. The advantages conveyed by its small size and market openness also mean that it can be easily swept up by developments beyond its shores (and control), particularly in light of the high rates of AI adoption.²⁰³ A further challenge posed by its small size means that Singapore has no inherent relevance globally with respect to technology development. While a jurisdiction with a large population size would be of interest to companies developing or deploying AI simply because of its economic heft and the amount of data it generates or stores, Singapore enjoys no such inherent advantage. Any relevance Singapore has on the global AI stage must first be earned; and once earned, maintained and nurtured assiduously.

87 At present, the *acquired* relevance Singapore has to the global AI ecosystems appears to centre around the notion of “trust”. The publicly available version of Singapore’s NAIS 2.0, for instance, mentions “trust” no less than 22 times. The notion of trust in an AI context is arguably an extension of Singapore’s *raison d’être* as a hub and intermediary for trade, business, finance and innovation throughout its history, and appears to be a sensible one. What this trust *entails*, and how to achieve it, however, is perhaps less clear. The publicly available edition of the NAIS 2.0 for instance, does not attempt to define or explain it; and it is uncertain if internal versions of the document do as well. Trust, after all, is an inherently nebulous, subjective and relational notion. In the context of AI, it will also evolve based on technological, industrial and regulatory change. While this paper is perhaps not the best place to explore the full contours of the notion of trust, what can be said is that from the perspective of developing regulatory regimes, any sensible notion of trust must holistically consider the entire AI business lifecycle,²⁰⁴ and take into account both the domestic and international environment.

202 Simon Chesterman, “From Ethics to Law: Why, When, and How to Regulate AI” (NUS Law Working Paper No 2023/014) (May 2023) at p 8 <https://law.nus.edu.sg/wp-content/uploads/2023/05/014_SimonChesterman.pdf> (accessed 22 December 2025).

203 “Singapore Leads Global GenAI Business Adoption, Customer Trust Trails Behind”, *Singapore Business Review* (2024) <<https://sbr.com.sg/hr-education/news/singapore-leads-global-genai-business-adoption-customer-trust-trails-behind>> (accessed 22 December 2025).

204 IT Modernization Centers of Excellence, US General Services Administration, “Solving Business Challenges with AI: Understanding and Managing the AI Lifecycle” in *AI Guide for Government* <<https://coe.gsa.gov/coe/ai-guide-for-government/understanding-managing-ai-lifecycle/>> (accessed 22 December 2025).

88 As regards the international environment, Singapore's reliance on foreign-developed AI solutions means that its regulatory regime must seek interoperability with the regulatory regimes in major AI-producing regions. For instance, Singapore can hardly afford insular regulations that diverge wildly from global norms. Doing so would risk shutting out investments or cutting-edge technologies, or creating unacceptable compliance hurdles for industry. The imperative, then, is to achieve a sensible and practical blend of alignment and autochthony: aligning regulatory frameworks with international standards to facilitate interoperability, while tailoring guardrails to safeguard the most crucial of domestic societal concerns and strategic interests. Its status as a small but advanced economy means policy coherence at home and compatibility abroad are both critical. Fortunately, Singapore's nimble governance and consultative law-making process (often involving industry and academia) position it well to achieve this dual imperative.

89 Notwithstanding this summary of Singapore's positioning and approach towards AI governance domestically and internationally, there remains room for improvement, as the next section will cover.

B. Opportunities for development

90 The authors argue that there are two dimensions of opportunities to further develop and hone Singapore's AI governance trajectory: international and domestic.

91 On the international front, the analysis of the three major developer jurisdictions above seeks to show the inherent complexity, and therefore opportunity, available to Singapore. While said in a different context, the words of veteran diplomat Bilahari Kausikan come to mind.²⁰⁵

Small countries are largely price takers in this complex world. But ... small countries are also never entirely without agency. This is precisely because of the inherent complexity of the foreign policy world that is defined by an endlessly shifting kaleidoscope of possibilities. Since the possibilities are in principle endless, there is always something that can be done – if only we have the wit to recognise it, and the courage to act on what we recognise. That is not to be taken for granted. But there is no action without risk. Sometimes the biggest risk is to try and avoid all risks.

92 Singapore retains further potential to punch above its weight in the global AI governance arena. One such avenue is by expanding its role

205 Bilahari Kausikan, "Issues and Problems in Singapore's Foreign Policy: Identity", *SSS@NTU Public Lecture Series* (14 November 2025) [YouTube Video] <https://youtu.be/NX_ObH6q9xs?si=uAdrRfO2m0frTJMa> (accessed 22 December 2025).

in the *development of technical standards and international frameworks for AI*. Rather than merely waiting to be shaped by rules set by others, Singapore can actively contribute to shaping them and seeding novel but credible ideas and pathways, leveraging its credibility as an honest broker between jurisdictions. A concrete example is the crosswalk between Singapore's AI Verify testing framework and the NIST AI Risk Management Framework.²⁰⁶ Such efforts enhance interoperability and demonstrate Singapore's capacity to foster international "common language" standards in AI governance. By continuing to champion initiatives like AI Verify, the Global AI Assurance Sandbox, and participating in global standard-setting (International Organization for Standardization/International Electrotechnical Commission ("ISO/IEC") committees, Institute of Electrical and Electronics Engineers ("IEEE") workshops, *etc*), Singapore can help build the bedrock of AI governance worldwide. Singapore can also provide and strengthen platforms for scientific and technical collaboration between the world's major developer jurisdictions, such as building on Singapore's hosting of the Singapore Conference on AI and the International Conference on Learning Representations.²⁰⁷ This not only raises Singapore's relevance, but also ensures that its interests – trusted access to data, regulatory interoperability, access to compute and AI capabilities – are reflected in global norms. In turn, this pre-positions Singapore firms to more easily navigate varying regulatory regimes, having been part of crafting the standards in the first place.

93 In the coming years, society can expect increasing emphasis worldwide on standardised evaluation of AI systems (for bias, safety, robustness, *etc*) and on certifications that signal trustworthiness. Singapore is well-placed to contribute to this trend. Its AI Verify testing toolkit, for instance, could be refined into a broader platform for AI validation, potentially recognised as a trusted testing corridor across countries. For businesses in Singapore, this could then mean a "test once, deploy globally" competitive advantage. In this regard, Singapore should drive efforts in the mutual recognition of testing frameworks and results. Further, as global consensus builds around certain norms (*eg*, the importance of AI model transparency or robust training data governance), Singapore should study incorporating these into its own

206 See para 45, n 101 above.

207 See Tharman Shanmugaratnam, President of the Republic of Singapore, "An Era of Possibility: Renewing Economic Order and Shared Purpose", lecture at the International Monetary Fund in Washington DC (15 October 2025) <<https://www.istana.gov.sg/Newsroom/Speeches/2025/10/25/An-era-of-possibility-Renewing-economic-order-and-shared-purpose-by-President-Tharman-Shanmugaratnam>> (accessed 22 December 2025).

regulatory framework, keeping its regime in lockstep with international best practices.

94 Domestically, there is room to bolster AI testing infrastructure and ecosystem testing capacity.²⁰⁸ While efforts have been made to foster a local AI testing community, these efforts to build a self-sustaining testing industry are still at a nascent stage. In this respect, the establishment of the Singapore AI Safety Institute (“AISI”) is a promising step. The AISI (anchored by the Digital Trust Centre at the Nanyang Technological University in partnership with IMDA) is tasked with advancing AI safety research, developing testing methodologies, and engaging in international collaborations on AI risk mitigation. Its mandate explicitly recognises that the science of AI safety and governance must keep pace with AI’s rapidly evolving capabilities. By driving technical work on AI evaluation and partnering with other global AI safety hubs, AISI will help Singapore stay at the frontier of understanding AI risks.

95 Further, as AI governance testing becomes increasingly commonplace, it may be an opportunity for Singapore to explore developing multi-disciplinary training pathways for individuals who are able to combine technical AI know-how and testing ability with knowledge of data or AI regulatory and compliance frameworks. Such individuals could help companies address the technical and regulatory challenges of AI testing.

96 Another area of opportunity lies in proactive planning for AI-related safety incidents as catalysts for improvement. No matter how robust the *ex-ante* regulatory framework, complex technologies like AI will inevitably produce unforeseen failures or accidents – whether it be a self-driving vehicle crash, a critical infrastructure outage caused by an AI decision, or a mass disinformation event triggered by generative AI. In other words, that there will be an AI-related global incident akin to the Black Thursday flash crash²⁰⁹ is what the late US Secretary of Defense Donald Rumsfeld called “known unknowns”.²¹⁰ In this regard, a leaf or two can be taken from Singapore’s experience during the COVID-19 pandemic, where Singapore’s effectiveness in handling the crisis in a pragmatic and transparent manner increased societal trust in Singapore’s public governance just as it fell in many other countries.

208 See para 41, n 84 above.

209 Simon Chesterman, *We, the Robots? Regulating Artificial Intelligence and the Limits of the Law* (Cambridge University Press, 2021) at pp 15–16.

210 Ella Lee, “Known unknowns’: Donald Rumsfeld’s Most Famous – and Infamous – Quotes”, *USA Today* (1 July 2021) <<https://www.yahoo.com/news/donald-rumsfelds-most-famous-infamous-192623597.html>> (accessed 22 December 2025).

(a) Firstly, Singapore should consider – and is in fact already considering – assurance-building mechanisms. One good example would be AI Verify. It would not be unforeseeable that should some crisis of confidence afflict AI systems, interest in AI assurance testing would spike. Singapore would then be well-placed to share its experience in running AI Verify to companies and jurisdictions globally.

(b) Secondly, Singapore can also consider having hard regulatory enablers. These are similar to “enabling” provisions in the AI laws of Japan and South Korea,²¹¹ which delegate powers to a particular government agency or committee to promulgate rules as and when they are needed.

(c) Thirdly, Singapore should treat such incidents (should they occur) not just as incidents to be managed, but as learning opportunities to strengthen the regulatory regime. This mindset mirrors the aviation sector’s evolution: each air incident is exhaustively investigated and often leads to new safety regulations, better training, or technological improvements, strengthening air safety over time. In the AI context, Singapore could establish protocols for AI incident reporting and investigation, as well as perhaps providing guidance to companies on how to analyse serious AI system failures. Insights gleaned can then feed back into regulatory adjustments or new guidelines (eg, stricter requirements on testing an autonomous vehicle’s algorithms if a flaw is discovered).

These suggestions take advantage of Singapore’s “regulatory soft power” of good inter-agency co-ordination, nimbleness and goodwill with industry to turn foreseeable crises into opportunity.

97 A third area of opportunity – as mentioned in para 40 above – is to enhance the ease of navigating the ever-growing thicket of guidelines, recommendations, frameworks and associated initiatives relating to AI in

211 See Arts 19–20 of the Act on the Promotion of Research and Development and the Utilization of AI-Related Technologies (Act No 53 of 2025) (Japan) <<https://www.kojimalaw.jp/wp/wp-content/uploads/2025/09/Japan-AI-Promotion-Act-KOJIMA-LAW-OFFICES-jp-en-reference-translation.pdf>> and Arts 7–8, Framework Act on the Development of Artificial Intelligence and Establishment of Trust (Law No 20676) (South Korea) <https://cset.georgetown.edu/wp-content/uploads/t0625_south_korea_ai_law_EN.pdf> (accessed 22 December 2025). See also Dominic Paulger, “Understanding Japan’s AI Promotion Act: An ‘Innovation-First’ Blueprint for AI Regulation”, *Future of Privacy Forum* (5 July 2025) <<https://fpf.org/blog/understanding-japans-ai-promotion-act-an-innovation-first-blueprint-for-ai-regulation/>> (accessed 22 December 2025).

Singapore. To date, the authors are aware of at least 11 such documents, ranging from the sector-agnostic to sector-specific. While admirable in demonstrating the government's technical and regulatory proficiency and proactiveness, this list risks causing most company decision-makers (especially in small and medium-sized enterprises) to shy away from AI governance. Put another way, this regulatory thicket risks turning efforts at regulatory clarity into regulatory confusion. To help industry navigate this tangle of initiatives, this paper proposes – at least as a first step – providing a one-stop avenue, perhaps pithily called “AI Governance Go Where”, to help organisations better understand how the various existing initiatives and guidelines are interconnected, and which initiative(s) an organisation should refer to for a particular purpose or objective. While such a facility may not make for as good a headline as a fresh set of guidelines, it would be an important step in helping provide greater accessibility and interpretability in AI governance to the broad mass of companies in Singapore.

98 A final opportunity lies in that of jobs. While the PDPC had published a *Guide to Job Redesign in the Age of AI* in 2020,²¹² that Guide was published pre-generative AI. Given how extensively new AI tools such as generative and agentic AI are now being used in enterprises, and the consequently heightened concerns about job displacement,²¹³ it only stands to reason that it would be timely for Singapore to reassess what job redesign should look like in an age of generative and agentic AI.

C. Navigating the dilemma of timing

99 The fast-evolving nature of AI technology means Singapore's regulators are inevitably confronted with the Collingridge dilemma:²¹⁴ early in a technology's lifecycle, it is hard to regulate due to limited understanding of its impact, but by the time impacts are clearer, the technology may be so entrenched that regulation becomes difficult or

212 *A Guide to Job Redesign in The Age of AI* (Infocomm Media Development Authority & Personal Data Protection Commission Singapore, 2020) <<https://file.go.gov.sg/ai-guide-to-jobredesign.pdf>> (accessed 22 December 2025).

213 See, for instance, Megan Wee, “Are Gen Z-ers in Singapore Worried about Generative AI Coming for Their Jobs?,” *The Straits Times* (4 August 2025) <<https://www.straitstimes.com/business/are-gen-zs-in-singapore-worried-about-gen-ai-coming-for-their-jobs>> (accessed 22 December 2025) and Anjli Raval, “The AI Job Cuts are Accelerating,” *The Straits Times* (5 August 2025) <<https://www.straitstimes.com/opinion/the-ai-job-cuts-are-accelerating>> (accessed 22 December 2025).

214 See Simon Chesterman, “From Ethics to Law: Why, When, and How to Regulate AI” (NUS Law Working Paper No 2023/014) (May 2023) at p 6 <https://law.nus.edu.sg/wp-content/uploads/2023/05/014_SimonChesterman.pdf> (accessed 22 December 2025).

disruptive. To navigate this classic problem, Singapore should adopt a regulatory posture that is flexible and forward-looking. In practice, this entails two strategies. Firstly, regulations and guidelines should be as technology-neutral as possible – focusing on the uses and effects of AI rather than specific technologies (which could quickly become obsolete). The PDPC’s MGF exemplified this by applying broad principles (eg, explainability, fairness, accountability) to a generic AI lifecycle while keeping the framework technology-agnostic. Such flexibility helps avoid over-regulating “yesterday’s AI” while missing new developments.

100 Secondly, Singapore should embrace an agile regulatory mindset – especially by utilising pilot programmes, regulatory sandboxes, policy co-creation with industry and other experimental policy tools. Regulatory sandboxes, in particular, offer a controlled environment where AI developers can test new technologies or business models under the regulator’s oversight and with certain legal exemptions. These mechanisms serve a dual purpose: they allow innovation to proceed (since participants get room to experiment without the full burden of compliance) while also yielding valuable data for regulators about real-world risks and appropriate safeguards. Building on existing regulatory sandboxes (as mentioned in para 43 above), Singapore can extend sandbox programmes to other high-impact AI domains (eg, healthcare) and use insights gathered to calibrate its regulatory responses. An agile regulatory mindset aligns with the views of scholars and experts like Simon Chesterman and Yeong Zee Kin, who have advocated for regulatory flexibility and “responsive regulation” for AI. Rather than attempting to craft perfect rules from the outset, it is more effective to start with guidance, monitor outcomes, and refine rules over time. Singapore’s relatively small size and strong public-private partnerships make it well-suited to this agile approach, as feedback loops between regulators and industry can be tighter and trust-based.

101 In essence, Singapore’s path through the Collingridge dilemma is likely to be a hybrid approach: starting with lighter, flexible governance, but being prepared to intervene decisively if and when clear evidence of harm emerges. By maintaining this balance, Singapore can adapt to technological change without either stifling innovation prematurely or finding itself reactive and overwhelmed later.

102 The future of AI governance for Singapore will be characterised by continuous evolution and collaboration. The country’s strategy should remain principled yet pragmatic – maintaining high-level commitments to trustworthy AI and public welfare, while nimbly adjusting tools and tactics as circumstances change. This turns back to the concept of *yin* and *yang* discussed at the start of this paper. Effective AI governance is not a one-off project but a continual and interdependent cycle. Rather

than seeking to find a single “correct” point of balance, or throwing sand into regulatory gears to moderate excesses of AI adoption, the answer lies in thoughtfully and consistently advancing aspects key to building the groundwork for international AI governance. In doing so, Singapore can serve as a model for how a small yet forward-looking nation can responsibly ride the wave of a technological revolution, maximising benefits for society while safeguarding core values and interests.
