

Asia Internet Coalition (AIC) Feedback to the public consultation on the draft Basic Law on Artificial Intelligence (“Basic Law”), Taiwan

19 September 2024

To,

The National Science and Technology Commission

The [Asia Internet Coalition \(“AIC”\)](#) express our sincere gratitude to the National Science and Technology Commission (NSTC), for the opportunity to submit comments on the public consultation on the draft Basic Law on Artificial Intelligence (“Basic Law”). The AIC is an industry association of leading Internet and technology companies. AIC seeks to promote the understanding and resolution of Internet and ICT policy issues in the Asia Pacific region.

We would like to commend the National Science and Technology Commission (NSTC) for drafting the Draft AI Basic Law. We support NSTC’s intent to promote the development of AI technology and application in Taiwan, and to build a trusted AI environment. We appreciate the NSTC’s well-rounded approach to promote the development of AI through public-private partnerships and international cooperation, without hindering the development of AI. **Please find below our detailed comments and recommendations, for your further consideration.**

We are grateful to the NSTC, for upholding a transparent, multi-stakeholder consultative approach and further welcome the opportunity to offer our inputs and insights, directly through industry meetings and participating in the official consultations / workshops.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact our Secretariat Mr. Sarthak Luthra at Secretariat@aicasia.org or at +65 8739 1490.

Thank you.

Sincerely,

Office of the Secretariat
Asia Internet Coalition (AIC)

Article in AI Basic Law (Draft)	Recommendation with Amendments	Explanation
Article 2 The term "artificial intelligence" as used in this Law refers to a machine-based system that has the ability to operate autonomously, and through input or sensing, through machine learning and algorithms, it can achieve predictions, contents, suggestions or decisions for explicit or implicit goals, and other outputs that affect the physical or virtual environment.	Article 2 The term "artificial intelligence" as used in this Law refers to a machine-based system that has the ability to operate autonomously, and through input or sensing, through machine learning and algorithms, it can achieve predictions, contents, suggestions or decisions for explicit or implicit goals, and other outputs that affect the physical or virtual environment <u>normally associated with human intelligence or perception</u>. <u>The term "end-user" means consumers or businesses using AI for personal use or enterprises using AI in a business context.</u> <u>The term "deployer" means a party who implements an AI system for use or who deploys the final system to the end-user.</u> <u>The term "developer" means a party who develops AI systems or software, or pre-trained models.</u> <u>The term "high risk artificial intelligence system" means an artificial intelligence system that when deployed makes decisions that have a material legal or similarly significant effect on the access of</u>	The definition of AI should be limited to the category of machine learning, as applications of ML are usually the applications that inspire transparency, bias, accountability, and accuracy considerations and therefore raise concerns from policymakers. As Recital 12 of the EU AI Act points out, the definition of AI should be "based on key characteristics of AI systems that distinguish it from simpler traditional software systems or programming approaches and should not cover systems that are based on the rules defined solely by natural persons to automatically execute operations". Algorithms should thus be excluded from this definition as it would render the definition of AI overly broad, sweeping in socially beneficial, low-risk, and everyday tools, such as calculators, calendar software, ticket scanners, and scantron machines. Excluding algorithms from the definition of AI would be consistent with international norms. For instance, the EU AI Act,¹ the US Executive Order on Safe, Secure, and Trustworthy Development and Use of AI

¹ EU AI Act, Article 3(1): 'AI system' means 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.

Article in AI Basic Law (Draft)	Recommendation with Amendments	Explanation
	<u>an individual to housing, employment, credit, education, healthcare, criminal justice or insurance.</u>	AI,² and the OECD's³ definition of AI all do not include "algorithms". Also, the technologies covered by the AI definition should be scoped to those that perform tasks "normally associated with human intelligence or perception", covering those activities undertaken with the goal of lacking human intervention. It is important that the AI Basic Law sets the overarching principles and standards that should apply universally, while government agencies tailor these principles to specific industry or application contexts. The underlying principle of what constitutes high-risk should be consistent across industries. In addition to adopting a risk-based approach to AI, it is thus also important for the AI Basic Law to establish the different roles in the AI value chain, and how responsibility is allocated between these roles.

² US Executive Order, Sec 3(b): The term "artificial intelligence" or "AI" has the meaning set forth in 15 U.S.C. 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.

³ OECD, "What is AI? Can you make a clear distinction between AI and non-AI systems?": An AI system is a machine-based system 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. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.

Article in AI Basic Law (Draft)	Recommendation with Amendments	Explanation
Paragraph 1 of Article 3 To promote the research, development and application of artificial intelligence, the government should take into account social welfare and digital equality in developing good governance and infrastructure, and follow the following principles:	Paragraph 1 of Article 3 To promote the research, development and application of artificial intelligence, the government should take into account social welfare and digital equality, <u>make reference to international or industry standards as well as best practices to support the</u> development of good governance and infrastructure, and follow the following principles:	Considering that artificial intelligence is still booming around the world, it is crucial that this draft is in line with international or industry standards and practices. Therefore, it is recommended that the provisions on research and development and application of artificial intelligence should refer to international or industry standards and best practices.
Paragraph 1(3) of Article 3 Privacy Protection and Data Governance: The privacy of personal data should be properly protected to avoid the risk of data leakage and the principle of data minimization should be adopted; at the same time, the opening and reuse of non-sensitive data should be promoted.	Paragraph 1(3) of Article 3 Privacy Protection and Data Governance: The privacy of personal data should be properly protected <u>and, where technically feasible, best endeavors should be used to reduce</u> to avoid the risk of data leakage and the principle of data minimization should be adopted; at the same time, the opening and reuse of non-sensitive data should be promoted <u>while taking into account important legal interests such as business secrets, personal data and information security</u>.	The importance of privacy and data governance principles should be recognized. However, this article does not define "non-sensitive information". Such ambiguity will make the application of regulations uneven and may also unduly affect the adoption and governance of AI. Furthermore, the Personal Data Protection Act has provided appropriate protection regarding the collection, use, processing, and international transmission of sensitive or non-sensitive personal data. In view of the fact that this draft is a high-level basic law, the principle of technology neutrality should be adopted. Accordingly, there should be no particularly stringent requirements for specific technical fields (i.e. artificial intelligence). To sum up, we

Article in AI Basic Law (Draft)	Recommendation with Amendments	Explanation
		suggest that the objects for data openness promotion and reuse should not be limited to non-sensitive data, so we recommend the modifications as shown on the left. In addition, it is recommended to amend the provisions to ensure that the legal text is consistent with the actual situation relating to data leakage risk control and data minimization.
Paragraph 1(5) of Article 3 Transparency and explainability: The output of AI should be appropriately disclosed or labeled to facilitate the assessment of possible risks and understand the impact on relevant rights and interests, so as to enhance the trustworthiness of AI.	Paragraph 1(5) of Article 3 Transparency—and—explainability: <u>Where technically feasible</u>, the output of AI should be appropriately disclosed or labeled <u>in high-risk AI use cases</u> to facilitate the assessment of possible risks and understand the impact on relevant rights and interests, so as to enhance the trustworthiness of AI.	At the outset, it is important to note that there are several different technical approaches to disclosure of synthetic media, including visible and invisible watermarking, cryptographic metadata, and fingerprinting (including of image, audio-, and audiovisual content), among other tools. We would encourage NSTC to consider that the state of the art will evolve and any future guidance related to labeling of synthetic content should be appropriately flexible to ensure that any such requirements are technically feasible. We also encourage that any guidance on labelling should take a risk-based approach and to focus on deployment scenarios where confusion about the origin of content could give rise to a material risk of harm. Since the requirement in paragraph 5 falls under the principle of transparency, which

Article in AI Basic Law (Draft)	Recommendation with Amendments	Explanation
		is different in nature from "explainability", it is recommended to adjust the text as shown on the left.
Paragraph 1(6) of Article 3 Fairness and non-discrimination: During the development and application of artificial intelligence, risks such as bias and discrimination produced by algorithms should be avoided as much as possible, and results that lead to discrimination against specific groups should be minimized.	Paragraph 1(6) of Article 3 Fairness and non-discrimination: During the development and application of artificial intelligence, risks such as bias and <u>improper</u> discrimination produced by algorithms should be <u>reduced avoided</u> as much as possible, and not cause results that lead to <u>improper</u> discrimination against specific groups should be minimized.	Bias detection and mitigation in data and model outcomes is fundamental for building responsible AI. Bias can be introduced in different ways; for example, imbalances in the training data may result in a model that is less accurate for certain subsets of the data. Bias may also be introduced by the machine learning algorithm itself—even with a well-balanced training dataset, the outcomes might favor certain subsets of the data as compared to the others. Rather than requiring that a training or production dataset must be free from bias, we recommend focusing on the importance of identifying and mitigating unwanted bias. The key questions are whether the model produces similar results across different groups (acceptable degrees of variation in performance/results depends on the use case) and if there is potential for harmful/unwanted impact. If there is too much disparity, deployers or users of a system will need to assess whether additional training or testing needs to be conducted and/or whether additional safeguards, such as human oversight, need to be implemented to ensure the outputs do not result in discrimination.

Article in AI Basic Law (Draft)	Recommendation with Amendments	Explanation
Article 9 The government shall avoid violations of relevant laws and regulations by applying artificial intelligence that causes damage to the safety, safety, freedom, or property safety of citizens, social order, or the ecological environment, or that causes conflicts of interest, deviations, discrimination, false advertising, misleading or falsified information. The Ministry of Digital Affairs and other relevant authorities may provide or propose tools or methods for evaluation and verification to facilitate the handling of the preceding matters by the competent authority of each purpose of the enterprise.	Article 9 The government shall avoid violations of relevant laws and regulations by applying artificial intelligence that causes damage to the safety, safety, freedom, or property safety of citizens, social order, or the ecological environment, or that causes conflicts of interest, deviations, discrimination, false advertising, misleading or falsified information. The Ministry of Digital Affairs and other relevant authorities may provide or propose tools or methods for evaluation and verification to facilitate the handling of the preceding matters by the competent authority of each purpose of the enterprise. <u>Such tools are to support the adoption of AI and should remain voluntary.</u>	In order to avoid creating regulatory and business uncertainty, MODA should be the only agency to take charge of developing evaluation tools in order to prevent inconsistent and overlapping testing frameworks from different agencies. We note that MODA has released a voluntary AI testing framework earlier the year 2024. We recommend that such testing frameworks should remain voluntary and that third-party audits for AI systems should not be implemented. Unlike cybersecurity and privacy, there is not currently a robust infrastructure for third-party independent audits in AI/ML. There is also currently a lack of consensus around the professional standards for AI system auditors and also no governing body ensuring baseline standards and imposing professional ethics. Encouraging robust internal, independent audits and controls, particularly at this stage, would strike an appropriate balance between providing meaningful safeguards while encouraging businesses innovation.
Article 10 The Ministry of Digital Affairs shall refer to the AI information security protection, risk classification and management developed	Not applicable	We noted that in the “Explanation” column of this Article, it is suggested that MODA will promote the AI risk classification framework with reference to international standards or norms, such as the EU AI

Article in AI Basic Law (Draft)	Recommendation with Amendments	Explanation
by international standards or norms, and promote an AI risk classification framework that is in line with international standards. The competent authority of each industry may follow the risk classification framework in the preceding paragraph to formulate the risk classification specifications for the industry it is in charge of.		Law which stipulate four levels of risks, including prohibited AI practices. We recommend MODA not to include a category of “unacceptable” or “prohibited” AI in the AI risk classification framework. First, by introducing a category of “prohibited” AI outright due to the belief that it is inaccurate or too risky, even in a voluntary assessment framework, will stifle innovation or development of better methods that can improve accuracy and reduce risk, which could otherwise ultimately enable the tech to societal benefits (e.g., to increase accessibility). This is because, while AI is at a nascent stage of development, it may be unclear to companies what sets a “prohibited” AI apart from a “high risk” AI. Companies may take an overly-cautious approach and decide not to invest in innovation, even if the technology could be used in low or medium risk applications with key benefits for users. Second, this is an approach that is currently uncommon among the AI regulatory frameworks that have emerged. For instance, we note that frameworks like the United States’ National Institute of Standards and Technology Risk Management Framework and Singapore’s AI Verify testing framework do not include such a category of “prohibited” AI.

Article in AI Basic Law (Draft)	Recommendation with Amendments	Explanation
		To the extent that the AI risk classification framework incorporates a concept of prohibited or unacceptable use cases, it is important that any such categories of “prohibited” AI must include an element of materiality in determining whether such AI presents material risk to individuals. Any “prohibited” AI use case should be very narrowly drawn and premised on social judgments that that use case is never going to be acceptable or there is no possible social benefit. If the concerns are that AI is not developed or accurate enough for certain use cases, then “high risk” would be the more appropriate bucket to continue responsible development and improvement of AI. In addition, any prohibition of the use of biometric identification systems and social scoring should, like the EU AI Act, be limited to public agencies, leveraging specific use cases presenting particularly high risk to the public.
Explanation of Article 10 To promote the research, development and application of artificial intelligence, the governments should take a risk-based approach and ensure the safe and stable operation of AI. In order to formulate artificial intelligence risk classification standards and operation verification	Explanation of Article 10 To promote the research, development and application of artificial intelligence, the government should take a risk-based approach <u>and should focus on specific use cases and usage scenarios to</u> ensure the safe and stable operation of AI. In order to formulate artificial intelligence risk	It is recommended to add “should focus on specific use cases and usage scenarios” in the explanation of Article 10, because by focusing on specific outputs, government agencies can make regulatory interventions in a focused manner rather than trying to regulate the rapidly developing computer science and deep learning technologies. This approach

Article in AI Basic Law (Draft)	Recommendation with Amendments	Explanation
mechanisms in line with international standards, the Ministry of Digital Development shall refer to international standards or norms to promote the artificial intelligence risk classification framework. For example, the EU AI Act stipulates four levels of risks, including prohibited AI activities, etc. Due to the different fields involved, the competent authorities of each industry may formulate risk classification and related management regulations based on the risk classification framework specified in the preceding paragraph.	classification standards and operation verification mechanisms in line with international standards, the Ministry of Digital Development shall refer to international standards or norms to promote the principle-based approach of the artificial intelligence risk classification framework. For example, the EU AI Act stipulates four levels of risks, including prohibited AI activities, etc. Due to the different fields involved, the competent authorities of each industry may formulate risk classification and related management regulations based on the risk classification framework specified in the preceding paragraph and international or industry standards.	grounds new rules on real issues and helps avoid overly broad regulations that could stifle broadly beneficial AI progress. In view of the fact that AI governance must consider the industry trend of continued development of AI, and conduct different governance according to individual usage scenarios, technologies involved, and risks involved, the risk classification framework referred to in this article should be a Risk-based Approach and should adopt a Principle-based Approach and Framework regulation in order to retain the flexibility of AI systems in various fields or individual application cases and to avoid difficulties in applications. Therefore, it is recommended to modify the explanation as shown on the left. Considering the interconnectedness of international trade and Taiwan's export-oriented economic and trade model, as well as the fact that artificial intelligence is still booming around the world, it is crucial to integrate with international or industry standards and implementation. Therefore, it is recommended to refer to the United States's NIST AI RISK MANAGEMENT FRAMEWORK and ISO/IEC 42001 and other specifications. As such, it is recommended to modify the second paragraph of the explanation as shown on the left.

Article in AI Basic Law (Draft)	Recommendation with Amendments	Explanation
Article 11 The Government shall identify, assess and mitigate the risks of the use of AI, and adopt standards, norms or guidelines to promote the development and application of AI, assess potential weaknesses and abuse situations according to the risk classification, so as to enhance the verifiability and human controllability of AI decision-making.	Article 11 The Government shall identify, assess and mitigate the risks of the use of AI, and adopt standards, norms or guidelines to promote the development and application of AI, assess potential weaknesses and abuse situations according to the risk classification and international standards , so as to enhance the verifiability and human controllability of AI decision-making.	For any standards, norms or guidelines relating to the use of AI, it is vital that we align around interoperable policy solutions to the greatest extent possible, and international standards, such as those set forth by ISO, play an important role. We promote regulating based upon international standards and definitions, so that we do not end up with a patchwork of local, conflicting standards, norms or guidelines. Such an outcome would undermine the potential of AI, particularly for small innovative companies in Taiwan that lack the resources to navigate a fragmented regulatory landscape. By developing standards in Taiwan that are aligned to international standards, companies in Taiwan will be able to offer their products and services globally.
Article 12 Based on AI risk classifications, governments should increase the trustworthiness of AI applications through mechanisms such as standards, verification, testing, marking, disclosure, traceability, or accountability, and establish relevant specifications for AI application conditions, liability, relief, compensation, or insurance, clarifying the	Article 12 Based on AI risk classifications and international standards , governments should help developers and deployers increase the trustworthiness of AI applications through mechanisms such as standards, guidance on best practices around verification, testing, marking, disclosure, traceability, or accountability, and establish relevant specifications for AI	The AI value chain is complex, with a single system often involving multiple developers, vendors, deployers, and users. Regulations should make clear who is responsible for compliance. We recommend clearly defining roles—for example, AI developers (i.e., those who develop AI systems or software, or pre-trained models), deployers (i.e., those who implement an AI system for use or who

Article in AI Basic Law (Draft)	Recommendation with Amendments	Explanation
attribution of responsibility and the conditions for attributing responsibility. In addition to complying with the basic principles of Article 3, the relevant norms of application responsibility in the preceding paragraph shall not be applied to any activities before the application of artificial intelligence technology development and research, so as to facilitate the development of technological innovation.	application conditions, and review and adjust relevant current regulations related to liability, relief, compensation, and insurance in accordance with the principles set out in Article 17, clarifying the attribution of responsibility and the conditions for attributing responsibility. <u>Government agencies should clearly assign responsibility for compliance to a specific actor (developers, deployers, end users).</u> In addition to complying with the basic principles of Article 3, the relevant norms of application responsibility in the preceding paragraph shall not be applied to any activities before the application of artificial intelligence technology development and research, so as to facilitate the development of technological innovation.	deploys the final system to the end-user), and end users (i.e., consumers or businesses using AI for personal use or enterprises using AI in a business context). Deployers of AI systems are best situated to assume most direct regulatory obligations as they are often most appropriately positioned to gauge, whether their use of a particular AI system will be high risk and identify mitigations appropriate for the context. As an example, in manufacturing and other software development, such deployers can require that developers and others within their supply chain make contractual commitments to demonstrate compliance for what they control or otherwise assist them with compliance. In addition, each participant should be able to handle liability, relief, compensation, insurance and other matters related to the use of artificial intelligence through current regulations or frameworks. If the current specifications or framework cannot fully consider the use of artificial intelligence, priority should be given to revising the relevant specifications or framework rather than formulating separate relevant frameworks that would lead to overlapping requirements.

Article in AI Basic Law (Draft)	Recommendation with Amendments	Explanation
Article 15 The government should establish mechanisms for data openness, sharing, and reuse, to increase the availability of data on the use of artificial intelligence, and periodically review and adjust relevant laws and regulations. The Government should strive to improve the quality and quantity of data on the use of AI in Taiwan, so as to ensure that the training results maintain the multicultural values of the country and safeguard intellectual property rights.	Article 15 The government should establish mechanisms for data openness, sharing, and reuse, taking into account important legal interests such as business secrets, personal data protection, and information security, to increase the availability of data on the use of artificial intelligence, and periodically review and adjust relevant laws and regulations. The Government should strive to improve the quality and quantity of data on the use of AI in Taiwan, so as to ensure that the training results maintain the multicultural values of the country and safeguard intellectual property rights.	For any mechanisms relating to data openness, sharing, and reuse, we recommend that training data of AI systems should not be required to be disclosed. Compilation of training data is a confidential commercial secret with significant competitive value. Requiring developers to disclose information about such data may foreclose the vendor's ability to claim trade secret protection under the law.