

China: New interim measures to regulate generative AI

In Brief

In recent months, generative artificial intelligence (**generative AI**) has taken the world by storm. Following plans to offer generative AI products announced by Chinese companies, the Cyberspace Administration of China (**CAC**) released on 11 April 2023 the [Measures for the Management of Generative Artificial Intelligence Services \(Draft for Comment\)](#) (**Draft Measures**) for public consultation. Following the consultation period, the [Interim Measures for the Management of Generative Artificial Intelligence Services](#) (**Interim Measures**) were published on 13 July 2023 and took effect on 15 August.

In contrast to the Draft Measures, the Interim Measures are a product of joint and coordinated efforts among seven key central government ministries / agencies, namely the CAC, the National Development and Reform Commission, the Ministry of Education, the Ministry of Science and Technology, the Ministry of Industry and Information Technology, the Ministry of Public Security, and the National Radio and Television Administration. The Interim Measures overall provide for more commercial and research-friendly conditions than those in the Draft Measures. In particular, some of the more onerous obligations on service providers in the Draft Measures have been removed from the Interim Measures, sending a positive signal to the business community that the development of and investment in generative AI technology and services is encouraged. The Interim Measures also acknowledge the possibility of foreign investment in developing and providing generative AI services in China, provided that the service complies with relevant laws.

This client alert provides an overview of the key provisions of the Interim Measures, the differences in China's regulatory approach compared to other jurisdictions and the potential implications of the Interim Measures for businesses operating in the generative AI service sector or engaging with generative AI service providers in China.

Background

In late May 2023, police in Baotou, in China's Inner Mongolia Autonomous Region, published details of an AI scam case in which the scammer used AI technology to create a fake face and voice in a video call that looked and sounded like the victim's real-life friend, tricking the victim out of CNY 4.3 million (USD 611,000). While this issue stemmed from "deep fake" technology rather than generative AI per se, the existence of the dangers relating to the unchecked use of AI are clear.

In light of this and similar stories and the increasingly dynamic nature of AI technologies, China has already been adopting a proactive, rather than a wait-and-see, approach in regulating AI. Under China's current AI regulatory framework, AI technologies are regulated by type. This contrasts with the approaches taken in other jurisdictions, such as the EU and US, which we discuss briefly below.

Following two sets of earlier regulations concerning AI recommendation algorithms (the Provisions on the Management of Algorithm Recommendations of Internet Information Services or "**Algorithm Recommendation Provisions**") and "deep fakes" (the [Administrative Provisions on the Management of Deep Synthesis of Internet Information Services](#) or

Contents

Background
Scope of application
Key obligations of service providers
Other obligations
Penalties
Analysis and key takeaways

"Deep Synthesis Provisions") respectively, which already have legal effect, the Interim Measures represent the latest element in the Chinese regulatory framework on AI, reflecting the Chinese government's intention to shape its own governance model. As with earlier Chinese regulations on AI, the Interim Measures similarly address issues of particular concern to the Chinese government, including security assessments, lawfulness of data sources, content moderation and algorithmic transparency.

The current regulatory model, while binding, will not be the end of the story, however. Further regulatory developments are already underway, including plans to enact an AI Law. The relevant bill is on the [State Council's 2023 legislative agenda](#), and while a draft has not yet been made public, China's current model of regulating by AI technology type could soon be replaced by an omnibus regime. Until then, however, generative AI users and service providers must comply with the Interim Measures as well as other related regulations and rules.

Scope of application

The Interim Measures apply to the use of generative AI technologies to provide services to the public in China. "Generative AI technology" is broadly defined as models and technologies capable of generating content such as text, images, audio, or video. It is unclear whether "the public" refers only to consumers (as opposed to services offered to businesses), although certain requirements appear to be targeting consumer-facing services.

The scope of application of the Interim Measures is narrower than what was originally proposed in the Draft Measures, which would have applied to both the research and development or use of generative AI products as well as the provision of services to the public in China. Aligning with this change is a new exception to the requirement to comply with the Interim Measures for industry associations, enterprises, education and research institutions, public cultural bodies and related professional bodies, etc. that simply research, develop and/or use generative AI technology without providing such services to the public. Such an approach underscores the authorities' support for organisations to coordinate their efforts in the generative AI field, push forward the establishment of data resources and encourage research and development in this area.

The Interim Measures impose various obligations on "generative AI service providers" ("**Service Providers**") (defined as organisations or individuals that use generative AI technology to provide generative AI services), which include those providing generative AI services through programmable interfaces (APIs), encompassing persons that provide the underlying technologies as well as those offering services at the application level.

Unlike the Draft Measures, which were silent on generative AI services provided from outside China, Article 20 of the Interim Measures explicitly states that when such services provided from outside China do not meet the requirements of or the Interim Measures or other Chinese laws or administrative regulations, the Chinese authorities can employ technical or other necessary measures to address such non-compliance (in practical terms this means blocking access in China to specific services). This suggests that it is possible for entities to provide generative AI services to China on a cross-border basis and that the Interim Measures in fact have a degree of extra-territorial effect.

Key obligations of Service Providers

Service Providers are subject to the following key obligations:

- Conducting **security assessments** in accordance with relevant existing regulations and filing certain information regarding the use of algorithms with the CAC in accordance with the Algorithm Recommendation Provisions, including the name of the service provider, form of service, algorithm type and an algorithm self-assessment report, **if generative AI services with "public opinion properties or social mobilization capacity" (undefined terms) are to be provided**
- Taking on the **responsibilities of a "personal information processor"** under the Personal Information Protection Law (PIPL) (similar to the concept of a data controller under the EU GDPR) where personal information is involved,

ensuring that personal data is obtained on the basis of consent, or in a manner that otherwise complies with the requirements of applicable Chinese laws and regulations, and refraining from collecting unnecessary personal information or illegally storing or sharing personal data

- Carrying out **pre-training, optimisation training and other activities handling training data** in accordance with the law, ensuring that:
 - the data and foundational models used have lawful sources;
 - the intellectual property rights of others are not infringed;
 - effective measures are employed to increase the quality of the training data, enhancing its truthfulness, accuracy, objectivity and diversity; and
 - the requirements of the Cybersecurity Law, Data Security Law, PIPL, and other related laws and regulations, are met.
- Taking **responsibility as the online information content producer** and fulfilling associated online information security obligations
- **Upholding core socialist values**, including not generating content that endangers national security, promotes violence and obscenity, is fake or harmful, etc.
- **Employing measures to address illegal content**, including stopping its generation and transmission, removing it, adopting model optimisation training and reporting to the relevant departments
- Employing measures to **address situations where users are found using generative AI services to engage in illegal activities**, including issuing warnings, limiting functionality and suspending or terminating the provision of services
- **Tagging the content created by generative AI** in accordance with the Deep Synthesis Provisions
- Adopting effective measures to **prevent discrimination** on the basis of ethnicity, religious belief, nationality, region, sex, age, profession, or health in the process of algorithm design, training data selection, model generation and optimisation, and service provision
- **Not endangering the physical and psychological well-being of others** and infringing their personal rights
- Employing effective measures to **increase transparency in the generative AI services**, as well as the accuracy and reliability of generated content (i.e. not just training data)

Other obligations

Other notable obligations to which Service Providers are subject include:

- Specifying intended users and uses of the service
- Adopting effective measures that prevent minors' over-reliance on and addiction to generative AI services
- Guiding users towards scientific understanding and lawful use of the generative AI technology

- Establishing mechanisms for user complaints and promptly handling them
- Addressing user requests regarding accessing, reproducing, modifying, supplementing or deleting their personal information
- Not using advantages in algorithms, data and platforms to engage in unfair competition

Penalties

Any violation of the Interim Measures will be penalised in accordance with the relevant laws and regulations of China, including without limitation the Cybersecurity Law, Data Security Law, PIPL and Law on Progress of Science and Technology, meaning that criminal sanctions can be meted out where the relevant acts constitute a crime.

Where the violation infringes public security, public security administrative sanctions will be imposed.

Where laws and regulations are silent, the CAC and other applicable regulators may issue warnings, order remedial actions to be taken within a specified period and, where the violator refuses to take remedial actions or the circumstances are serious, order suspension of the related services.

The provision permitting the CAC to impose fines from RMB 10,000 to 100,000 (USD 1,380 to 13,800) in the Draft Measures has been removed from the Interim Measures.

Analysis and key takeaways

Relative commercial friendliness of the Interim Measures

The Interim Measures are generally more commercially friendly than the Draft Measures given the removal of certain onerous obligations. For example, the requirement for the Service Providers to adopt measures to filter inappropriate or unlawful content created by generative AI, and to optimize algorithms to prevent the repeated generation of such content within three (3) months of receipt of notice has been replaced by a more general obligation to report and adopt measures for addressing such issues.

Some obligations retained in the Interim Measures are also not new in China. For example, the security assessment requirement exists in the Provisions on the Security Assessment of Internet Information Services With Public Opinion Properties or Social Mobilization Capacity in relation to Internet Information Service Providers that meet one of several conditions. The obligation to address excessive reliance or addiction to AI content in the Interim Measures echoes similar rules under the Algorithmic Recommendation Provisions.

Principles like non-discrimination, transparency, privacy or personal data protection, intellectual property and trade secrets protection, as well as respect for other lawful rights and interests enshrined in the Interim Measures are also seen in AI laws and draft regulations elsewhere in the world. The training data handling requirements in Article 7 of the Interim Measures generally align with international standards, for example the requirement in the EU AI Act for high-risk AI systems that make use of techniques involving the training of models with data to be developed on the basis of training, validation and testing data sets that meet certain quality criteria.

However, uncertainties remain around the implementation of these training data requirements in practice. For example, Article 19 requires Service Providers to provide information on the sources, models, types, tagging rules, algorithm mechanisms, etc. for training data to the relevant government departments but it does not specify what supporting documents would be deemed sufficient. Further guidance on these issues would be helpful to facilitate effective implementation.

Things Service Providers should watch for

- The broad range of liabilities for Service Providers under the Interim Measures - it is possible that upstream AI developers could be held liable for issues arising from the acts of downstream companies that utilise their generative AI tools, in the same way that users may have a right of action against upstream suppliers in product liability claims. The issue of allocation of liability would need to be addressed in contracts between developers and companies providing services to the public. In addition, an end user can report a Service Provider to the CAC if the generated content does not comply with the requirements of the Interim Measures.
- The obligation to apply to the CAC for a mandatory security assessment would create a barrier to entry for certain Service Providers, though such obligation only exists where the service carries a “public opinion property” or “social mobilisation capacity”. These concepts are included in various existing China regulations including the Provisions on the Security Assessment for Internet-based Information Services with Public Opinion Property or Social Mobilization Capacity, and which are defined to include “information services such as forums, blogs, microblogs, chat rooms, communication groups, public accounts, short videos, webcasts, information sharing, small programs, etc.... and other Internet-based information services that provide channels for the public to express their opinions or are capable of mobilizing the public to engage in specific activities.” On this basis, a generative AI service that provides **output that reveals the opinion of a person or a group of people, or that provides suggestions to users on what actions to take would likely fall within the definition and thus be subject to a security assessment.**
- The requirement to ensure that the data and foundational models used have lawful sources could create practical difficulties for assembling a sufficiently large training data set usually required for developing a successful generative AI model. Whether the input data is subject to intellectual property protection (and how to obtain clearance for those rights) could be hard to ascertain. The obligation in Article 7(4) on Service Providers to take “effective measures” to increase the quality, truthfulness, accuracy, objectivity and diversity of training data may be difficult to monitor and enforce.
- The obligations concerning the protection of individual rights are extensive. It may be impossible, impractical or costly in certain cases for Service Providers to have to obtain consent from data subjects to the use of their personal data to train the model where there is no other clear legal basis, and technically challenging to comply with individual requests made by data subjects for modifying or deleting their personal data used in a data set for training the generative AI. As with the draft EU AI Act, which does not refer specifically to the requirement of consent to collection of personal data in the context of generative AI datasets, the legal basis will fall to be assessed in accordance with existing data privacy laws.

Contrast with the regulatory approaches of other jurisdictions

China has been active in enacting legislation to address AI and its by-use-case approach contrasts with other jurisdictions.

The EU AI Act is a piece of prescriptive, product safety legislation that seeks to provide a structure for day-to-day AI lifecycle management. It will be applicable generally to the development, trade and use of AI-driven products, services and systems across different sectors within the EU. Instead of regulating AI technologies by type, different requirements apply to AI systems depending on their level of risk. AI practices posing unacceptable risks are prohibited, while at the other end of the spectrum, AI systems with low and minimal risks are not subject to any obligations. AI systems with high risk and limited risk fall in the middle. A new European AI Office is to be established and will be responsible for implementing the EU AI Act, by issuing opinions, recommendations and guidance.

Unlike the EU's more prescriptive and “horizontal” (or “cross-sectoral”) approach, the UK intends to adopt a principles-based and sectoral approach in regulating AI. Rather than regulating AI through legislation, it has issued a **white paper** outlining five principles that UK regulators should consider to best facilitate the safe and innovative use of AI in the sectors they oversee, namely (1) safety, security and robustness; (2) transparency and explainability; (3) fairness; (4) accountability and governance; and (5) contestability and redress. There will not be a specific AI regulator. Rather, existing regulators in different industries will provide guidance on using AI within their remits based on the five principles,

e.g. [guidance](#) from the Information Commissioner's Office on AI and data protection and the [Software and AI as a Medical Device Change Programme](#) introduced by the Medicines and Healthcare products Regulatory Agency, which seeks to ensure that patients are protected.

The US, on the other hand, appears to be taking a wait-and-see approach in regulating AI. While AI-specific laws exist in a number of states and certain existing federal and state laws address aspects of AI, such as privacy, security and anti-discrimination, there is currently no comprehensive federal AI legislation. Though some new and proposed frameworks have been issued by various federal agencies and an increasing number of states are considering laws addressing various uses of AI-enabled technology, a clearer and more consistent AI regulatory plan has yet to emerge.

It remains to be seen how China's approach shapes the development and use of generative AI in the country and whether it serves to encourage the development of this ground-breaking technology.

Contact Us



Isabella F.C. Liu

Partner

Isbella.Liu@bakermckenzie.com



Dominic Edmondson

Special Counsel

Dominic.Edmondson@bakermckenzie.com

© 2023 Baker & McKenzie. **Ownership:** This site (Site) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms, including Baker & McKenzie LLP). Use of this site does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All information on this Site is of general comment and for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulation and practice are subject to change. The information on this Site is not offered as legal or any other advice on any particular matter, whether it be legal, procedural or otherwise. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any information provided in this Site. Baker McKenzie, the editors and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents of this Site. **Attorney Advertising:** This Site may qualify as "Attorney Advertising" requiring notice in some jurisdictions. To the extent that this Site may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. All rights reserved. The content of the this Site is protected under international copyright conventions. Reproduction of the content of this Site without express written authorization is strictly prohibited.

