中倫律師事務所
ZHONG LUN LAW FIRM

Deciphering the AIGC Compliance Blueprint (Part II): Record-filing for AIGC Algorithm

Peng Cai

1. INTRODUCTION

As a vital part of AIGC governance, algorithm record-filing serves as a regulatory tool to enforce the legal requirements of algorithmic transparency. Its primary objective is to safeguard user rights by ensuring product and information security. Since the introduction of the requirements for algorithm record-filing by the *Internet Information Service Algorithmic Recommendation Management Provisions* ("Algorithm Provisions") and the *Internet Information Service Deep Synthesis Management Provisions* ("Deep Synthesis Provisions"), the Cyberspace Administration of China ("CAC") has consecutively released four rounds of domestic internet information service algorithm record-filing lists, along with the first algorithm record-filing list for domestic deep synthesis services.

In alignment with the requirement of algorithm record-filing, major application stores have initiated a pre-launch review of AIGC-related applications to ensure compliance. Per Article 13 of the Deep Synthesis Provisions, if an AIGC product fails to meet the legal requirement of algorithm record-filing, application stores have the remit to take actions including denying shelf space, issuing warnings, suspending services, or even removing the application from the stores. As Part II in a series of articles intended to chart the regulatory course for AIGC and explore its potential trajectory under the current legal advancements, this article seeks to guide readers through the complexities of the algorithm record-filing process, a step that AIGC product developers cannot miss if they want to successfully bring AIGC products to the market.

2. THE DISTINCTION BETWEEN "DEEP SYNTHESIS ALGORITHMS" AND "GENERATIVE SYNTHESIS ALGORITHMS"

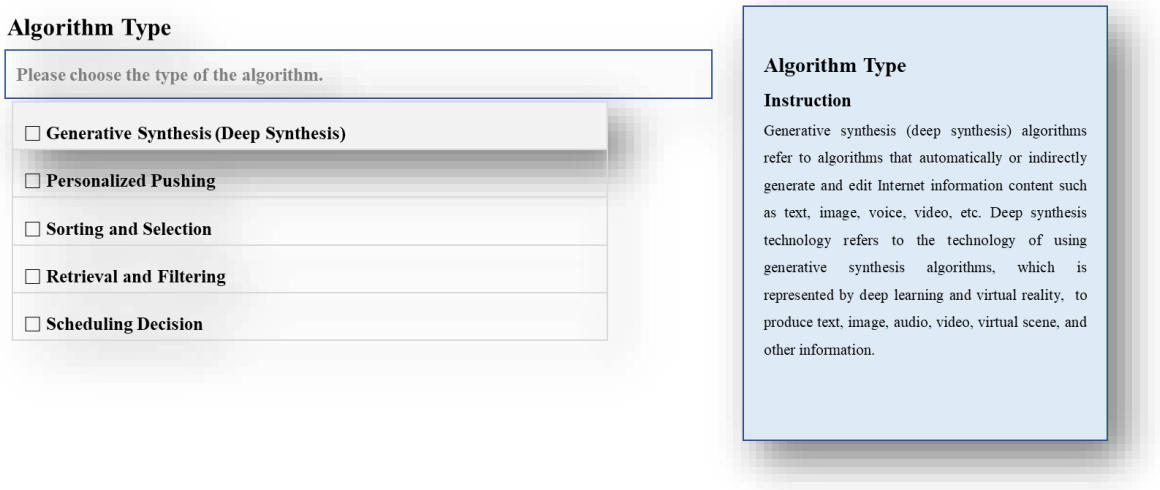
After the release of the Deep Synthesis Provisions, distinctions between "deep synthesis algorithms" and "generative synthesis algorithms" have been widely discussed among all stakeholders in the AIGC industry. While deep synthesis algorithms and generative

synthesis algorithms each exhibit their unique characteristics, the underlying similarity underscores the association between them. For instance, both deep synthesis algorithms and generative synthesis algorithms apply advanced deep learning technologies such as convolutional neural networks (CNN), generative adversarial networks (GAN), variational autoencoders (VAE) to generate diverse forms of content and data, and both find versatile applications in fields including but not limited to computer vision, image processing, computer graphics, virtual reality, and augmented reality.

Notably, the key difference lies in the respective outputs of these two types of algorithms. Deep synthesis algorithms specialize in generating novel data that closely mirror the real-world counterparts. A well-known example is the deepfake technology, which generates hyper-realistic images or videos by "swapping" faces. In contrast, generative synthesis algorithms aim to generate completely original content based on pre-defined rules, parameters, or models, thereby presenting an even more natural rendition of the "reality", like "creating" new facial images from scratch.

The fundamental commonality between deep synthesis algorithms and generative synthesis algorithms lies in their capacity to create content that significantly diverges from existing reality. Both leverage the power of deep learning to understand, learn, and mimic the intrinsic characteristics of data, thus generating new data that is seemingly realistic and convincing. As a result, despite their distinct approaches – "swapping facial appearances" or "creating facial images" - both technologies ultimately serve the same purpose of pushing the boundaries of what's achievable in data generation. Hence, in terms of regulatory compliance such as algorithm record-filing, businesses are not obliged to differentiate between the two technologies.

Following is the actual filing interface. For the "Algorithm Type" row, readers can find that procedurally, the CAC treats generative synthesis (AIGC) and deep synthesis algorithms the same under one filing section:



3. STEP-BY-STEP GUIDANCE ON ALGORITHM RECORD-FILING

Given that the CAC has not established a distinct record-filing procedure for generative synthesis algorithms and considering the unique nature of the deep synthesis algorithms—which necessitates a specific role-identification for the filing entity—we will introduce the entire record-filing process using the deep synthesis algorithm as an illustrative example.

(1) Record-filing Entity

The roles inherent to deep synthesis algorithms include deep synthesis service provider and deep synthesis service technical supporter, with each bearing distinct responsibilities during the record-filing of the same algorithm. Entities should consider the following guidelines to discern their record-filing responsibilities:

- If an entity takes up both roles for the same algorithm, it must independently fulfill the record-filing process as both a deep synthesis service provider and a deep synthesis service technical supporter.
- If an entity solely functions as a deep synthesis service provider without offering technical support, it shall complete the record-filing merely as a deep synthesis service provider.
- If an entity procures deep synthesis technology from a supplier and utilizes this technology to deliver deep synthesis services to end-users, it must independently meet its record-filing obligation as a deep synthesis service provider, regardless of the supplier's record-filing status.

Within a corporate group where multiple subsidiaries might share algorithms, the group can designate the subsidiary that controls the algorithm as the record-filing entity. However, if the algorithm record-filing entity differs from the ICP record-filing entity for the same AIGC product, the algorithm record-filing entity may be required to provide an explanation detailing the relationship between these two entities and reasons for this discrepancy.

(2) Recording-filing Process

Per the record-filing guidance issued by the CAC in alignment with the Deep Synthesis Provisions, and considering our previous project experience, the record-filing procedures for AI algorithms can be delineated into three steps:

- Step 1 - Information of the Record-filing Entity. Relevant information regarding the record-filing entity should be submitted. Once manually approved by the CAC, the record-filing entity can proceed to submit the data regarding the algorithm and the functionality of the AIGC products.
- Step 2 - Information of the Algorithm. Following Step 1, required information regarding the algorithm should be submitted during the record-filing as follows:

basic information required for the algorithm

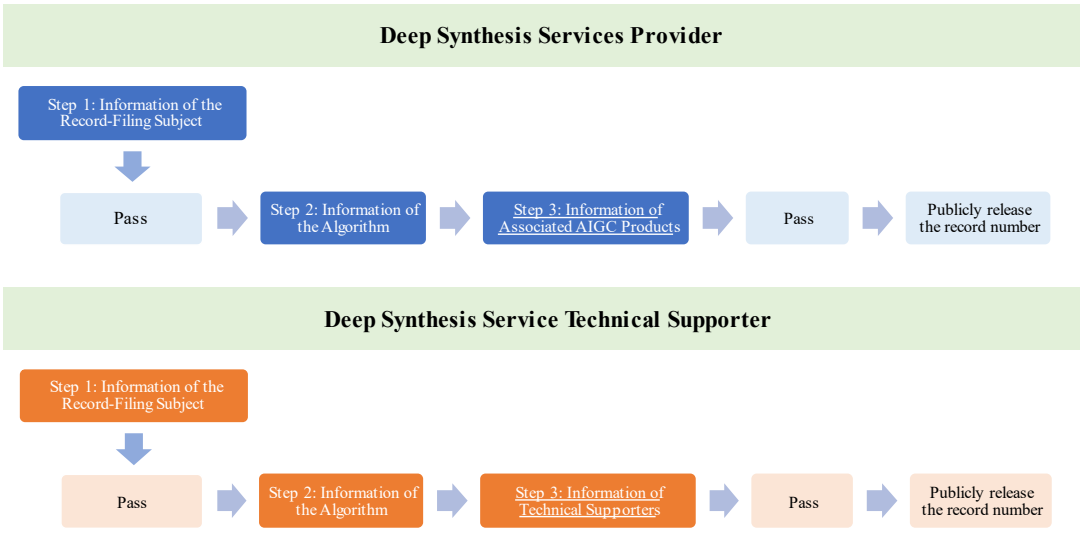
Algorithm Type	Please choose the type of the algorithm.
Algorithm Name	Please type in the name of the algorithm.
Launch Time	Please choose the date.
Application Area	Please choose the application area.
Self-assessment Report of Algorithm Security	Please upload the self-assessment report of algorithm security.
Text to Be Publicized	Please upload the text to be publicized.

detailed information required for the algorithm

Algorithm Introduction	Please type in the introduction of the algorithm. (No more than 200 words.)
Usage Scenario	Please choose the usage scenario.
Algorithm Data	
Input Data Modality	Please choose the input data modality.
Does the input character feature include biometric features?	☐ Yes. ☐ No.
Does the input character feature contain identity information?	☐ Yes. ☐ No.
Output Data Modality	Please choose the output data modality.
Output File Format	Please choose the output file format.
Output File Size	Please type in the output file size.
Does the algorithm support batch output?	☐ Yes. ☐ No.
Algorithm Model	
The Source of Training Data	
Does the training data include overseas data?	☐ Yes. ☐ No.
How to generate training data?	Please choose the mechanism to generate training data.
Does the training data involve personal information?	☐ Yes. ☐ No.
Generative Synthesis Algorithm Type	Please choose the type of the generative synthesis algorithm.
Algorithm Hardware Requirements	Please type in the type of the algorithm hardware requirements.
Algorithm Performance	Please type in the algorithm performance.
Algorithm Calculation Method	Please choose the algorithm calculation method.
Algorithm Strategy	
Do you preprocess the training data? (model strategy)	☐ Yes. ☐ No.
Do you preprocess user input data? (input strategy)	☐ Yes. ☐ No.
Do you post-process the output results?	☐ Yes. ☐ No.
Risk of Algorithm and Prevention Mechanism	
Do you attach implicit identification to the generated synthesized content created	☐ Yes. ☐ No.

by your service?	
Do you attach significant identification to the generated synthesized content?	☐ Yes. ☐ No.
Do you have the capacity to remind users to prominently identify the generated synthesized content?	☐ Yes. ☐ No.
Security Guarantee Mechanism for User Data	Please choose the security guarantee mechanism for user data.
Refutation Mechanism for Generative Synthesized Fake Information	Please choose the refutation mechanism for generative synthesized fake information.
Discovery and Disposal Mechanism for Generative Synthesized Harmful Content	Please choose the discovery and disposal mechanism for generative synthesized harmful information.
Explanation of Risk Prevention Mechanism	Please type in the explanation of risk prevention mechanism. (No more than 200 words.)

- Step 3 – Information of Associated AIGC Products and Technical Supporters. The record-filing process requires different information from the deep synthesis service provider and the deep synthesis service technical supporter, primarily during Step 3. The deep synthesis service provider is expected to provide details about associated AIGC products and their functionalities, while the deep synthesis service technical supporter should provide information about the technical support plan. The summary of the submission process for the deep synthesis service provider and the deep synthesis service technical supporter is as follows:



Owing to the extensive information required during the record-filing process, we advise businesses to prepare the required content in advance by utilizing the Internet Information Services Algorithm Record-Filing System provided by the CAC.

(3) Record-filing Documents

During the algorithm record-filing process, besides inputting the basic and detailed information aforementioned, entities are also required to prepare the following documentation:

- Table for Implementation of Responsibility of Algorithm Security. As part of Step 1, a record-filing entity is expected to upload the completed table to demonstrate compliance. This document should detail the dedicated algorithm security department within the entity, in addition to the algorithm security management policies they adhere to. These policies should include but are not limited to the algorithm security self-assessment policy, algorithm security monitoring policy, algorithm security violation penalty policy, emergency response policy, and the policy for ethical review of technology.
- Algorithm Security Self-assessment Report. In Step 2, entities should submit an algorithm security self-assessment report detailing the operations of the algorithm, including but not limited to, specific information about the algorithm (workflow, data, model, and intervention strategies), its application in service, risk assessment, risk control measures, and security evaluation conclusions. Specifically, deep synthesis service providers are expected to provide additional information regarding content governance, generated content marking, rumor debunking mechanisms, and user rights protection.
- Proposed Public Disclosure. Pursuant to the Algorithm Provisions, providers of algorithm recommendation services are obliged to disclose the core principles, objectives, and operation mechanisms of their services appropriately. During Step 2 of the record-filing process, entities should submit their proposed public disclosure information, primarily encapsulating the algorithm's core principles, operation mechanisms, application scenarios, and objectives. While the CAC has not specified detailed requirements for public disclosure, we suggest entities adhere to the existing industry standards to fulfill the obligations of algorithm disclosure without revealing trade secrets or technical know-how concerning the

algorithm.

The aforementioned documents are crucial for the success of completing an algorithm record-filing process. They not only cover the technical aspects of the algorithm but also explore the depth of the algorithm compliance structure, including security management systems, organizational constructs, and risk mitigation strategies. Therefore, we strongly recommend that entities initiate strategic planning and thorough preparation for the algorithm record-filing process well ahead of time. Engaging external legal experts can significantly facilitate the preparation of record-filing materials in an efficient, comprehensive, and timely manner.

4. RECORD-FILING DEADLINE

In accordance with the Algorithm Provisions, upon successful submission of all requisite information and documents pertaining to algorithm record-filing, the CAC is obligated to finalize the record-filing process within thirty working days. But entities should be aware that, based on our first-hand project experience, the record-filing process for algorithms may last as long as more than two months, given the likelihood of back-and-forth revisions and subsequent re-submissions.

5. CONCLUSIONS

The recent *Interim Measures for the Management of Generative Artificial Intelligence Services* requires completion of the algorithm record-filing process of AIGC services and products before they enter the market. Entities should commence this process promptly as it takes time and involves a comprehensive internal review of algorithms, requiring painstaking preparation of necessary documentation on the entities' part. Entities should consider engaging external legal consultants that are familiar with relevant regulations and practical procedures and should also maintain up-to-date communication with regulatory bodies. After the record-filing is completed, entities must conspicuously display their record-filing number and disclose algorithmic principles and operations.