Application, Risks, and Policies of Generative AI

Huang, JenChih |
Research Associate, The Second Research Division

The autonomous creative capability of "Generative Artificial Intelligence" (referred to as Generative AI) has become a significant emerging technology influencing the socio-economic landscape. Open AI's ChatGPT has gained widespread attention and application, representing a breakthrough in Generative AI and showcasing its immense creative autonomy on a global scale. Currently, numerous tech startups and businesses have developed dedicated services in various fields through the integration of application programming interfaces (APIs). These applications include writing articles, creating visual and audio content, generating design solutions, crafting marketing copies, and coding, to name but a few. These applications are gradually transforming the operations of socio-economic activities.

However, even with its convenient usability and creative ability, Generative AI has also raised several concerns in practical applications. These concerns include the harm caused by malicious use and the provision of erroneous information leading to making unappropriated decisions. Additionally, Generative AI poses three significant risks that deserve attention:

(1) Aggravating the digital divide in society: amplifying the market power of individuals who possess and control AI technologies.

(2) Increasing forgery risks: Deepfakes and false information generated by Generative AI make the general public more vulnerable to fraud.

(3) Impact on social ethics, morality, and law: Questions arise regarding the attribution of creative outputs generated by Generative AI. Will biases or discrimination in its pre-training data and algorithms be amplified through its applications? How should the severity of criminal intent and liability be measured when illegal activities are assisted by Generative AI?

Therefore, it is vital to propose governance strategies for AI applications. The European Commission has formulated a "Regulatory framework proposal on Artificial Intelligence," which categorizes AI applications into different risk levels and provides regulations and transparency requirements for each level. The UK's "Artificial

Intelligence White Paper: New World Leading Approach to AI in the UK " presents five regulatory principles to promote innovative AI applications, including (1) safety, security, and robustness; (2) transparency and explainability; (3) fairness; (4) accountability and governance; (5) contestability and redress. The US's "An Implementation Plan for a National Artificial Intelligence Research Resource " proposes an integrated portal to support AI developers with the research tools and services they require, aiming to lower barriers to participating in the AI research ecosystem. It also adopts two pilot strategies: the open pilot (NAIRR-Open) and the secure pilot (NAIRR-Secure).

In summary, Generative AI brings users valuable creative outputs, but the content does not always originate from evidence-based reasoning, which is a key characteristic and issue in current Generative AI applications. The associated risks of malicious intent and deepfakes have become important governance topics in the development of Generative AI. Referring to the strategic perspective of the UK, USA, and EU, two crucial issues should include: building the ecosystem and platforms required for AI innovation and designing mechanisms to deal with different types of risks. Recently, Taiwan's National Science and Technology Council has also proposed a draft of Taiwan's "Basic Law on Artificial Intelligence" based on these considerations. However, with the widespread proliferation of Generative AI applications abroad in daily life, it would be critical to evaluate how Taiwan’s academics and startups can generate technological alternatives, and whether regulatory measures can assist the public in coping with the related impacts and risks. Further empirical investigations are needed.