LOS ANGELES & SAN FRANCISCO

Daily Journal

www.dailyjournal.com

TUESDAY, DECEMBER 19, 2023

GUEST COLUMN

A green light for EU AI Act

By Robert Spano, Emily Lamm and Hayley Smith

In a historic development, on Dec. 8, 2023, EU legislators reached political agreement on the Artificial Intelligence Act ("AI Act"), representing a monumental step forward in the realm of AI regulation.

The AI Act is the most significant attempt to design a comprehensive legislative framework for regulating AI, and due to its extra-territorial effect, is poised to have far-reaching implications for companies *globally* (not just those based in the EU) if they do business in the Union.

The law establishes obligations for AI depending on its potential risks and level of impact on fundamental rights. Certain applications of AI are banned outright, while high-risk AI is subject to the most stringent obligations. It is expected that the AI Act will formally come into force early next year, after which companies will be given two years (until early 2026) to fully comply with the new legislation. Companies must take heed and carefully assess whether they are within the scope of the AI Act and, if so, take appropriate steps to prepare for compliance.

What's covered?

At its core, the AI Act classifies AI systems based on risk – unacceptable risk (which are prohibited), high-risk (which are subject to burdensome obligations), low risk (which are subject to limited transparency requirements) and finally, minimal risk (which carry no obligations). Examples of prohibited AI systems include AI used to exploit the vulnerabilities of people or manipulate human behavior to circumvent free will, AI used for emotion recognition in the workplace and educational institutions, and most AI used for real-time remote biometric identification for law enforcement purposes in publicly accessible spaces. On the flipside, AI systems that are used solely for research and innovation, for military or defense purposes, or by individuals for non-professional reasons are expressly excluded from coverage.

The AI Act identifies AI systems as "high risk" if they pose a significant risk to an individual's health, safety, or fundamental rights, and are used, or intended to be used, in certain critical areas, such as education, employment, critical infrastructure, public services, law enforcement, border control, and administration of justice. Such AI systems are subject to a comprehensive set of thorny compliance requirements such as the establishment of a risk-mitigation system, provision of technical documentation, diligent record-keeping, completion of a conformity assessment (to ensure harmonized standards are met), and the completion of a mandatory fundamental rights impact assessment, among other requirements. However, in response to concerns that common, low-risk uses of AI would be classified as high-risk, thereby leading to the stifling of innovation, EU legislators agreed on a filter system to exempt AI systems that are intended to perform low-level (e.g., procedural) tasks from the high-risk category.

Although not initially part of the AI Act, the emergence of generative AI tools like ChatGPT in the public's consciousness ultimately led to general purpose AI models (or foundation models) to be within the scope of the law. These models are subject to a tiered regulatory approach that imposes more substantial obligations on those deemed to pose "systemic risks." Such obligations include reporting energy consumption, undertaking red-teaming exercises, signing a code of conduct, and ensuring adequate cybersecurity controls. However, the regulation of foundation models has been the subject of much debate (with some EU Member States pushing back entirely) and ambiguity as to the exact scope and content of the rules lingers. For instance, there is uncertainty regarding the technical benchmarks and qualifying thresholds for foundation models, with resolution expected to hinge upon the Commission adopting secondary legislation. Additionally, the concept of red-teaming remains unclear for companies as there is no further explanation in the current text.

Enforcement framework

The enforcement of the AI Act is

Robert Spano *is a partner, and co-chair of the Artificial Intelligence Practice Group, and* **Emily Lamm** *and* **Hayley Smith** *are associates at Gibson, Dunn & Crutcher LLP.*

set to be spearheaded by a centralized European AI Office, which will be responsible for enforcing binding rules upon AI. This centralized approach aims to streamline enforcement efforts and ensure a consistent application of the regulations.

Enforcement will be implemented in a staggered manner. While the majority of the law is anticipated to be enforceable in approximately two years, prohibitions on banned AI systems will already be in effect six months after the Act is finalized. Furthermore, the rules governing general-purpose AI systems will apply in about 12 months.

Non-compliance with the AI Act carries significant consequences. Maximum fines can reach up to €35 million or, in the case of a company, up to 7% of the total worldwide annual turnover for the preceding financial year, whichever is higher. However, specific fine amounts corresponding to concrete obligations have not been disclosed, adding an element of uncertainty to the penalty landscape.

What should you do next?

Although the final text of the AI Act is yet to be published, there is sufficient information available for companies to initiate the compliance planning process. Navigating the complexities of the AI Act requires a proactive and informed approach. By monitoring developments, understanding the nuances of risk classification, implementing tailored compliance measures, and preparing for enforcement, companies can position themselves to not only meet regulatory requirements but also thrive in the evolving landscape of AI governance.