CEP Magazine - August 2023

Robert Bond (robert.bond@privacypartnership.law) is Senior Counsel with Privacy Partnership Law in the United Kingdom and Immediate Past President of SCCE & HCCA.

The European Union's smart (or not so smart) way to regulate artificial intelligence

By Robert Bond, BA, CCEP, CITP, FSALS, CompBCS

In 2020, the European Commission published its white paper "On Artificial Intelligence – A European approach to excellence and trust."[1]

The white paper begins by stating, "Artificial Intelligence is developing fast. It will change our lives by improving healthcare (e.g., making diagnosis more precise, enabling better prevention of diseases), increasing the efficiency of farming, contributing to climate change mitigation and adaptation, improving the efficiency of production systems through predictive maintenance, increasing the security of Europeans, and in many other ways that we can only begin to imagine. At the same time, artificial intelligence (AI) entails a number of potential risks, such as opaque decision-making, gender-based or other kinds of discrimination, intrusion in our private lives or being used for criminal purposes."

Proposed AI Act

In 2021, the European Union (EU) unveiled the world's first proposal to regulate AI and reign in "high-risk" uses of AI, including facial recognition or job application software, that in the EU's view, might lead to potential threats to society and individuals (AI Act).[2] Specific objectives of the AI Act are to:

- Ensure that AI systems placed on the EU market and used are safe and respect existing law fundamental rights and EU values;
- Ensure legal certainty to facilitate investment and innovation in AI;
- Enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems; and
- Facilitate the development of a single market for lawful, safe, and trustworthy AI applications and prevent market fragmentation.

The AI Act proposed that AI systems will be regulated based on their potential to cause harm by creating three risk categories: "low," "high," and "unacceptable."

- Low-risk systems are those that pose no risk to fundamental rights and freedoms.
- High-risk systems are those that pose significant risks to the health, safety, or fundamental rights and freedoms of humans.

- Unacceptable-risk systems are those that pose a serious threat to fundamental rights and freedoms and, as such, are banned.

Businesses have been concerned that without a clear definition of high risk, many organizations could more easily breach the law. Moreover, the AI Act may stifle technology innovation in the EU.

Applicability and impact of the AI Act

The AI Act is intended to apply to any business that puts AI or uses AI on or in the EU market and so is extraterritorial in its reach. More than that, the AI Act will integrate with and coexist alongside existing legislation, such as the General Data Protection Regulation, the Digital Services Act, and the draft Cyber Resilience Act.

The recently announced revised Product Liability Directive, sitting alongside the AI Act, introduces new EU rules on liability that will affect product supply chains—particularly where they incorporate software or AI as a key component.

Standalone software and AI systems will be defined as "products" such that claimants may be able to apply for compensation where defective products cause them harm. In addition, such products will be considered defective if they do not address cybersecurity standards.

The organizations that the new Product Liability Directive catches include not only manufacturers but also importers and distributors. Potentially, authorized representatives and digital service providers that facilitate trade between vendors and customers of defective products will be liable.

These proposed laws and regulations will affect all sectors, including life sciences and technology.