ALERT

DOJ Debuts Updates to Its Evaluation of Corporate Compliance Programs Aimed at the Responsible Use of Artificial Intelligence

By Tony Phillips, Johnna Purcell

TAKEAWAYS

- On September 23, 2024, the U.S. Department of Justice (DOJ) updated its Evaluation of Corporate Compliance Programs (ECCP) guidance to instruct prosecutors on how to evaluate corporate risk related to the management and use of emerging technologies, such as artificial intelligence (AI).
- Utilizing the new guidance, prosecutors will now evaluate whether a corporation has appropriately considered the risks associated with technologies, such as AI, and if it has taken sufficient steps to mitigate the risks associated with these technologies.
- The guidance is instructive for companies utilizing AI in their operations or that may be vulnerable to AI-powered criminal schemes. Such companies should ensure they have structured compliance programs to withstand scrutiny by the DOJ in the event they are subject to an investigation.

10.08.24

On September 23, 2024, the U.S. Department of Justice (DOJ) Criminal Division released an updated version of its Evaluation of Corporate Compliance Programs (ECCP) guidance. DOJ first published the ECCP in 2017 to provide clear guidance on which factors federal prosecutors will consider when evaluating the strength of a corporation's compliance programs in the context of an investigation or enforcement action. The ECCP instructs prosecutors on how to evaluate a company's risk assessment mechanisms, to ensure that the company's policies and procedures are responsive to the risks that it has identified and communicate those risks, and the established risk mitigations, to the corporation's stakeholders, such as employees and vendors. The ECCP is a critical resource that companies should consider when developing compliance programs to avoid penalties associated with DOJ enforcement action.

In March 2024, Deputy Attorney General Lisa Monaco requested that the DOJ Criminal Division "incorporate assessment of disruptive technology risks, including risks associated with AI" so that prosecutors could "assess a company's ability to manage AI-related risks as part of its overall compliance efforts." This guidance is the latest in a variety of executive actions aimed at regulating the use of AI by bolstering the security of the technology and protection of users.

ECCP Guidance on AI

The ECCP guidance incorporates the framework for defining AI outlined in the Office of Budget and Management directive on Advancing Governance, Innovation and Risk Management for Agency Use of Artificial Intelligence. The ECCP guidance specifies that "no system should be considered too simple to qualify as a covered AI system due to a lack of technical complexity" and that AI includes even the use of smaller models that were trained on small subsets of data. Thus, machine learning developed and trained only using a corporation's own data would likely still qualify as AI for the purpose of this guidance and be scrutinized accordingly.

The guidance instructs prosecutors to consider whether companies have adequately considered the risk that new and emerging technologies may pose to their ability to comply with criminal laws when evaluating a corporation's risk assessment processes. In particular, regarding the use of AI, the guidance instructs that adequate risk assessments should consider whether the corporation has:

- a mechanism by which it can assess the impact of AI to comply with criminal laws;
- considered the management risk related to the use of AI within the broader context of its enterprise risk management;
- governance and compliance polices related to the responsible use of AI;
- considered the risks that reckless or deliberate misuse of technologies such as AI by insiders could have to their operations and whether they have implemented policies and controls responsive to these risks;
- considered what is the baseline of human decision making used to assess any AI-generated content including, but not limited to, monitoring for bias or inaccuracy; and
- developed and implemented appropriate training to ensure that employees understand the responsible use of AI and other emerging technologies.

In her remarks announcing the guidance, Principal Deputy Assistant Attorney General and head of DOJ Criminal Division Nicole Argentieri stated that prosecutors will use the new guidance to assess how corporations manage risks "related to the use of new technology such as artificial intelligence both in their business and in their compliance programs." Thus, investigations under the new guidance will appear to be two-fold and assess both how a company is using AI in its own operations and how a company's interactions with external AI may expose vulnerabilities.

So, for example, a DOJ evaluation under the new ECCP guidance may concern how the use of AI by a company's employee might make it vulnerable to violating its own internal policies, such as its code of conduct. But an ECCP evaluation may also consider whether a company is vulnerable to criminal schemes that utilize AI generated content or images. Corporate risk assessments and polices are expected to account for vulnerabilities related to its own use of AI within the organization and the use of AI by others outside the organization.

Implications for Compliance Programs

Given the new DOJ guidance, corporations should assess their own compliance programs to ensure that they have adequately considered the risks that AI and similar emerging technologies may pose to their operations, and companies must implement policies and controls to adequately address those risks. Companies should begin by assessing how AI or other emerging technologies do or could affect their operations. Companies should be sure to investigate within their operations teams to determine if and how their employees may be utilizing AI to perform their functions. Companies will also want to consider how their operations may be vulnerable to manipulation by AI tools. If companies utilize AI or other emerging technologies even in minor ways, they should ensure they have considered the risks associated with such use, craft policies to protect against those risks, and develop and implement training to educate their employees regarding both the risks and applicable policy.