CLIENT ALERTS & INSIGHTS

DOJ Adds AI Considerations to Its Evaluation of Corporate Compliance Programs

OCTOBER 8, 2024

Authors: Shaneeda Jaffer, Juan Mata, Ryan J. Levitt

Last month, the U.S. Department of Justice's ("DOJ") Criminal Division announced its periodical update to its Evaluation of Corporate Compliance Programs ("ECCP"), zeroing in on how companies manage risk related to artificial intelligence (AI) and other "disruptive" technologies.

The DOJ's Eye on AI

The development of artificial intelligence presents a watershed moment for government investigators and non-governmental compliance professionals alike. AI technology will continue to reinvent how regulatory authorities and, consequently, compliance professionals approach risk management. For the DOJ, the ECCP has been a key tool to encourage changes in corporate compliance programs.

The ECCP update relies on the Office of Management and Budget (OMB)'s definition of AI in Memo M-24-10 to capture, generally, any system that is designed to (1) learn from experience and improve performance when exposed to data sets, or (2) approximate a cognitive task, act rationally, or mimic how a human thinks or acts. Although the DOJ has stated that there is no complexity floor for a system to be considered an AI system, for the ECCP, systems are not AI if they only have "robot process automation," exhibit behavior "defined only by human-defined rules," or learn purely through the repetition of "an observed practice exactly as it was concluded."

The DOJ has honed in on AI since February when Deputy Attorney General Lisa Monaco labeled AI as having the "sharpest blade" of any "double-edged sword." She also said that prosecutors would "seek stiffer sentences for offenses made significantly more dangerous by the misuse of AI." Last Monday's announcement regarding updates to compliance, governance, and risk assessment systems comes as no surprise.

Stressing the Risk of AI in the ECCP

The DOJ's updates include, for the first time, extensive guidance on evaluating and managing risks as a company uses AI and other emerging technologies. The ECCP revisions make clear that an effective compliance program that accounts for AI risk should, at minimum, include:

- Assessments of risks presented by AI and other emerging technologies in day-to-day commercial operations and in the compliance program itself;
- Risk assessments and other compliance measures with sufficient financial resources and breadth of relevant data sources; and

- Access to the same resources and technology to gather and leverage data for compliance purposes that a company is using in its business.

Evaluating AI in Compliance

In conjunction with the ECCP updates, the head of the DOJ's Criminal Division, Nicole Argentieri, remarked that prosecutors will consider:

- The technology that a company and its employees use to conduct business, whether the company has conducted a risk assessment of the use of that technology, and whether the company has taken appropriate steps to mitigate any risk associated with the use of that technology; and
- Whether the company is monitoring and testing its technology to evaluate if it is functioning as intended and consistent with the company's code of conduct.

Applying the DOJ's Revisions to the ECCP

Companies under investigation by the DOJ will need to demonstrate that they have robust compliance programs for any AI in use either for commercial or compliance purposes.

Examples of AI in the compliance landscape could include:

- **Horizon Scanning**: quickly scanning and evaluating the ever-evolving regulatory landscape, including pending legislation, enforcement actions, proposed rules, and public comments by regulators, to predict future developments, risks, and concerns.
- **Regulatory Change Management**: monitoring active regulatory obligations and daily change alerts to reduce the need for the manual and tedious review leading to improved reaction and adoption times.
- **Internal Controls:** analyzing large data sets, identifying trends, and detecting control failures, to streamline internal controls.

AI systems have a breadth of applications, and naturally, they vary by industry. Their value-add to an organization's compliance efforts, regardless of industry, will only grow in years to come, and so will the regulation around emerging technologies. As the shortcomings of manual compliance operations grow with the advent of new legislation and regulatory guidance, AI systems can step in to improve outcomes while controlling costs.

Companies can refer to the January 2023 National Institute of Standards and Technology (NIST) AI Risk Management Framework for further information on how to conduct risk assessments of their use of AI and emerging technologies to conform to the ECCP revisions. At Benesch, we provide fulsome reviews and updates of our clients' compliance programs, including analyzing their use and management of AI systems. Companies should not ignore the potential rewards and risks of using or ignoring AI in their compliance programs. After all, the DOJ's message is emblematic of the modern

state of the compliance field: make the necessary compliance investments to help prevent, detect, and remediate misconduct - or face the consequences.

For more information, please contact a member of Benesch's White Collar, Government Investigations, and Regulatory Compliance Practice Group.

Shaneeda Jaffer at 628.201.0793 or sjaffer@beneschlaw.com.

Ryan Levitt at 312.517.9550 or rlevitt@beneschlaw.com.

Juan Mata at 312.212.4944 or jmata@beneschlaw.com.