Westlaw Today

Recent updates to the DOJ's evaluation of corporate compliance programs

By Peter V.B. Unger, Esq., Alexander S. Birkhold, Esq., and Elizabeth Satarov, Esq., ArentFox Schiff LLP*

DECEMBER 6, 2024

This past September, the US Department of Justice (DOJ) updated its Evaluation of Corporate Compliance Programs (ECCP). The revised guidance reflects the government's evolving expectations regarding corporate responsibility and compliance efforts, especially concerning artificial intelligence (AI) and emerging technologies.

The key updates concern: (1) risks associated with new technologies and AI, (2) leveraging data for compliance program monitoring and enhancements, and (3) whistleblower protections. These revisions, and a brief background on the ECCP, are discussed below.

Background

The DOJ published the ECCP in 2017 as guidance for prosecutors for the evaluation of a company's corporate compliance program. The ECCP identified several hallmarks of an effective corporate compliance program, which were accompanied by a set of questions for each hallmark that were meant to assist prosecutors in the review of these programs.

The updated ECCP includes guidance on how to manage risks related to the use of new technologies, such as AI, in a corporate- and compliance-related setting.

The ECCP was created only as guidance and not as rigid standards that companies must follow, understanding that each company has a different risk profile and solutions for reducing risk. However, through the ECCP, the DOJ clearly put emphasis on the importance of a comprehensive and effective compliance program that can detect and deter misconduct. The full description of the DOJ's hallmarks can be found here: https://bit.ly/41l04AH.

The DOJ has continued to update the ECCP since 2017, expanding its application to the entire Criminal Division of the DOJ, expanding guidance on acquisitions, adequate resourcing, and utilizing data, and adding guidance on communication, messaging, and use of personal devices. The most recent updates to the ECCP are outlined below.

New technologies and AI

The updated ECCP includes guidance on how to manage risks related to the use of new technologies, such as AI, in a corporate- and compliance-related setting. The DOJ states that the definition of AI encompasses, but is not limited to, the AI technical subfields of machine learning (including, but not limited to, deep learning as well as supervised, unsupervised, and semi-supervised approaches), reinforcement learning, transfer learning, and generative AI.

The ECCP outlines a number of questions that a company should assess regarding AI and new technologies, which include:

(1) Does the company have a process for identifying and managing emerging internal and external risks that could potentially impact the company's ability to comply with the law, including risks related to the use of new technologies?

(2) How does the company assess the potential impact of new technologies, such as AI on its ability to comply with criminal laws?

(3) Is management of risks related to use of AI and other new technologies integrated into broader enterprise risk management (ERM) strategies?

(4) What is the company's approach to governance regarding the use of new technologies such as AI in its commercial business and in its compliance program?

(5) How is the company curbing any potential negative or unintended consequences resulting from the use of technologies, both in its commercial business and in its compliance program?

(6) How is the company mitigating the potential for deliberate or reckless misuse of technologies, including by company insiders?

(7) To the extent that the company uses AI and similar technologies in its business or as part of its compliance program, are controls in place to monitor and ensure its trustworthiness, reliability, and use in compliance with applicable law and the company's code of conduct?

(8) Do controls exist to ensure that the technology is used only for its intended purposes? What baseline of human decision-making is used to assess AI?

(9) How is accountability over use of AI monitored and enforced?

(10) How does the company train its employees on the use of emerging technologies such as AI?

In order for a company to begin assessing whether they are able to answer these questions regarding new technologies and AI, a company must understand how these technologies are used internally. They must assess their industry-specific AI and technology risks and their tolerance for such risks. They then must monitor, evaluate, and test how AI and new technologies are used and whether they are functioning as intended and if they are consistent with the company's code of conduct.

In addition, the ECCP advises companies to conduct risk assessments of these technologies and provides the January 2023 National Institute of Standards and Technology AI Risk Management Framework as a resource. To learn more about the legal implications of AI in a variety of industries view our comprehensive AI Industry Guide (here: https://bit.ly/41iCeW9) and our AI Law Blog (here: https://bit.ly/3ZEXOlB).

Leveraging data

In recent years, the DOJ has emphasized the growing importance of data in corporate compliance programs and in detecting, preventing, and mitigating potential misconduct. The government is even using data analytics to proactively identify potential foreign bribery (https://bit.ly/3TXZXFU). Moreover, SAP, the German-based software company, was credited for its data analytics capabilities in its January 2024 settlement (https://bit.ly/3D1BA5C) with the DOJ.

Building on this trend, the revised ECCP also stresses the importance of using data analytics to evaluate the effectiveness of a compliance program. This information should be leveraged to evaluate different risks areas, like third-party relationships. In addition to using data to create efficiencies in compliance operations, the information should be used to improvements to the compliance program.

The compliance function should also have access to different data sources in a reasonably timely manner. The updated ECCP stresses that a company should understand and manage the quality of its different data sources. Additionally, prosecutors are instructed to consider whether there is an imbalance between the technology and resources used by the company to identify and capture market opportunities and the technology and resources used to detect and mitigate risks.

Data is expected to play a bigger role in compliance programs. Many companies would benefit from developing procedures to help compliance personnel collect and understand data related to compliance. This information should then be harnessed to improve the compliance program.

Whistleblower protections

Throughout 2024, the DOJ has emphasized its commitment to incentivizing whistleblowing and supporting whistleblower protections. In March, the DOJ announced a new whistleblower program (https://bit.ly/3ZizSEi) that will provide financial rewards to individuals who notify the DOJ of misconduct. Then in August, it released (https://bit.ly/4dnlK1d) additional guidance on the program and emphasized its commitment to vigorously investigate and prosecute federal criminal offenses.

In recent years, the DOJ has emphasized the growing importance of data in corporate compliance programs and in detecting, preventing, and mitigating potential misconduct.

The ECCP's recent updates highlight the DOJ's focus on whistleblowing. The updated guidance asks protectors to evaluate, among other factors:

- Whether the company has an anti-retaliation policy.
- Trainings for employees concerning internal anti-retaliation policies and external anti-retaliation and whistleblower protection laws.
- The manner in which the company disciplines employees involved in misconduct who actually reported the misconduct compared to others involved in the misconduct but who did not report it.

The DOJ also continues to examine the way companies encourage and incentivize reporting potential misconduct or violation of company policies. It also expects companies to assess its employees' willingness to report misconduct.

Companies should assess whether they have implemented sufficient internal reporting hotline mechanisms to incentivize employees to bring potential misconduct to the company's attention rather than make external reports. Importantly, companies should also ensure they have implemented appropriate anti-retaliation policies and conducted trainings that align with the updated ECCP.

About the authors



Peter V.B. Unger (L) is a partner in the litigation group at **ArentFox Schiff LLP**. He concentrates on defending clients in governmental investigations, including actions before the Securities and Exchange Commission, Department of Justice and Congress. He is based in Washington, D.C., and can be reached at peter.unger@afslaw.com. **Alexander S. Birkhold** (C) is a partner who counsels clients on global ethics and compliance strategies, cross-border investigations, and white collar prosecutions. He is located in Los Angeles and can be reached at alexander.birkhold@afslaw.com. **Elizabeth Satarov** (R) is an associate in the firm's New York office. Her practice is focused on government and internal investigations, global ethics and compliance counseling, and white collar criminal and civil litigation. She can be reached at elizabeth.satarov@afslaw.com. This article was originally published Nov. 15, 2024, on the firm's website. Republished with permission.

This article was published on Westlaw Today on December 6, 2024.