The Promise and the Peril: AI and Disruptive Technologies in Operations and Compliance

Compliance and Ethics

Technology, Privacy, and eCommerce

Banner artwork by MangKangMangMee / *Shutterstock.com*

In September 2024, the US Department of Justice (DOJ) revised the Evaluation of Corporate Compliance Programs (ECCP) to incorporate consideration of a company's management of artificial intelligence (AI) and other disruptive technologies when a federal prosecutor weighs charging and resolution decisions. Regardless of where on the maturity spectrum a company is with respect to AI and disruptive technologies, the ECCP update provides an indispensable guide to building or enhancing risk-mitigation and risk-management tools to respond to the DOJ's perception of the risks these technologies pose in operations and compliance. This article provides some general strategies and tactics for companies to consider in light of the new guidance.

Since its rollout in 2017, the DOJ and others have used the ECCP as the criterion against which to assess compliance programs. The ECCP is not prescriptive or proscriptive; rather, it articulates a series of inquiries to assist a prosecutor with determining whether a company has an effective compliance program. Nor does the ECCP forecast a one-size-fits-all approach; context matters. Including the September 2024 update, the DOJ has revised the ECCP four times to address enforcement priorities and emerging topics.

For example, the 2024 update largely focuses on AI and disruptive technologies, recent DOJ self-disclosure initiatives, and the compliance function's access to corporate data sources. In each of these areas, the DOJ previewed elements of the update through its other initiatives. In a February 2024 speech, Deputy Attorney General Lisa Monaco announced the AI Justice Initiative through which the DOJ sought to embrace the "promise" of AI by increasing its understanding and use of AI while confronting the "peril" of AI by announcing more robust enforcement and penalties for AI-involved offenses.

The ECCP defines AI by reference to the Office of Management and Budget memorandum "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence" (AI Memo). AI is any artificial system that:

1. "Performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets,"

2. "Solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action,"

3. "Think[s] or act[s] like a human,"

4. "Is designed to approximate a cognitive task," or

5. "Act[s] rationally."

The AI Memo provides technical context to assist with understanding the definition of AI. AI includes machine learning, reinforcement learning, transfer learning, and generative AI. AI "includes systems that are fully autonomous, partially autonomous, and not autonomous and systems that operate both with and without human oversight." AI does not include automated processes pursuant to human-designed rules or learning achieved solely by repetition. The AI Memo highlights, though, that no system is too simple to be an AI system.

Explore more leading-edge practices at the 2025 ACC Cybersecurity Summit.

AI and disruptive technologies in operations

Although prior ECCP iterations focused almost exclusively on the compliance function, the 2024 update also addresses how operations confront AI and disruptive technologies. Now, prosecutors are to "consider the technology — especially new and emerging technology — that the company and its employees are using to conduct company business." In addition, they are to ask what actions the company is taking to "curb[] any potential negative or unintended consequences" and to "mitigat[e] the potential for deliberate or reckless misuse of technologies." Finally, prosecutors will ask, "How does the company train its employees on the use of emerging technologies such as AI?"

To meet the guidance, a company could consider taking at least four steps. The order of these steps will depend on the maturity of a company's AI awareness and governance. The below order reflects a company in an immature state that wants to triage its exposure before investing in consistent governance tools that might take longer to develop.

1. A company needs to understand its business operations' AI use. To gain this knowledge, a company could conduct an inventory of the use of AI and disruptive technologies across the enterprise. Given the prevalence of AI — both formally and informally used by business operations — a thorough inventory may pose challenges, and a company should design the inventory with this

diffuse use of AI and disruptive technology in mind.

2. After conducting an inventory, a company should perform a use-case analysis to ascertain whether each use aligns with its expectations from a business-process perspective and from a financial perspective.

3. A company should implement AI governance. An acceptable-use policy is an important step to corralling exposure and limiting the risks of a bring-your-own-AI environment. Additionally, identifying a person or persons responsible for AI governance is important to ensure consistent application of the company's approach to AI and disruptive technologies.

4. A company should train operational personnel on the acceptable use of AI and disruptive technologies as well as the approval process for new AI and disruptive technology adoption.

Malign use of AI

In addition to considering a company's own AI use in operations, the DOJ will assess a company's exposure to malign use of AI against the enterprise's interest by insiders or outsiders. The DOJ likely will weigh the following types of considerations as part of that assessment:

- Examination of algorithmic collusion and exclusionary practices (i.e., whether AI algorithms are designed or used in ways that could facilitate unlawful collusion or exclusionary practices);
- Perpetuation of bias and discrimination (i.e., whether the AI systems perpetuate unlawful bias or discrimination in a way that produces harmful outcomes, particularly in areas impacting individuals' rights and opportunities);
- Openness and understandability (i.e., the transparency of AI systems and whether individuals are aware of AI interactions);
- Robustness and security (i.e., whether the systems are designed to be safe and can be overridden or repaired if they cause harm);
- Accountability and risk management (i.e., the traceability of their outputs and the application of systematic risk management throughout the AI lifecycle); and,
- Cybersecurity safeguards and protocols (i.e., evaluating disaster recovery plans, access controls, and training programs to mitigate AI-related threats).

Although the above inventory process can be a good start to this exposure analysis, a company should also evaluate how its other systems may be exposed to misuse of AI or other disruptive technologies. Some top risks related to the use of AI systems include privacy and confidentiality risks, disinformation, cyber threats, bias and ethical concerns, intellectual property/copyright issues, accuracy and reliability, and security vulnerabilities.

Companies can guard against these risks by:

- Avoiding input of personal information and other sensitive, confidential, or proprietary data into AI systems;
- Developing policies that define acceptable use and require oversight of AI systems (as well as proper vetting of the AI systems before implementing their use);
- Using real-time auditing tools to track and validate the authenticity of the AI-generated data;
- Training employees;
- Developing and regularly updating incident response plans and disaster recovery plans; and
- Establishing a governance structure to oversee AI systems and confirm responsible use.

AI and disruptive technologies in compliance

The 2024 ECCP update suggests that a compliance function should respond to AI and disruptive technologies both defensively and affirmatively. Interestingly, one could read the ECCP to be the DOJ's articulation that all AI risk governance should be housed in the compliance function, although in practical terms, significant coordination with other relevant corporate functions would likely be required for effective AI risk governance.

Compliance function defensive posture to AI

The update sets an expectation that a company will, among other steps, evaluate the company's use of AI and disruptive technologies in its risk assessment. A prosecutor will ask whether "management of risks related to use of AI and other new technologies [is] integrated into broader enterprise risk management (ERM) strategies." From the risk management process, a prosecutor will ask what "controls [are] in place to monitor and ensure [AI's] trustworthiness, reliability, and use in compliance with applicable law and the company's code of conduct."

> The update sets an expectation that a company will, among other steps, evaluate the company's use of AI and disruptive technologies in its risk assessment.

The National Institute of Standards and Technology (NIST) has developed an AI Risk Management Framework (AI RMF) to guide organizations in assessing and managing risks associated with AI systems. This framework is designed to enhance the trustworthiness of AI technologies and is intended for voluntary use by organizations. The NIST AI RMF is based on core principles of governance, mapping, measuring, and managing risks in AI. It aims to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems. The AI RMF encourages ongoing monitoring and periodic review of AI systems to ensure they meet intended objectives and to integrate measurable continuous improvement activities into system updates.

Compliance function affirmative use of AI

The DOJ, though, does not expect the compliance function to merely have a defensive posture with respect to AI; rather, the DOJ anticipates that the compliance function could leverage AI and

disruptive technologies in at least two affirmative ways. First, the DOJ expects that the compliance function could leverage AI in its compliance work. Second, the DOJ expects that the compliance function could use AI in its self-assessment processes.

AI in compliance work

A compliance function's affirmative use of AI in its work can vary in scope and sophistication. For example, AI could have a role in compliance education, compliance testing, and investigations.

Compliance education

An AI chatbot can field initial inquiries about whether an action complies with company policies. A company should only release such a chatbot after rigorous testing to ensure accuracy, to build the chatbot's knowledge base, and to prevent hallucinations. In addition, the chatbot should identify the relevant policy references that informed its response and advise the requester of their responsibility to ensure compliance with policy. Such a chatbot may free up limited human resources in the compliance function, allowing it to dedicate scarce resources to other priority needs.

Compliance testing

AI could have a central role in expanded compliance testing. AI excels at processing large volumes of data and identifying either patterns or anomalies that a compliance staffer might miss in manual review. In addition, because of its scale, AI could allow the compliance function to conduct more testing than manual or other processes would have performed in the past.

Investigations

AI may help expedite investigations. Natural language processing can:

1. Quickly digest voluminous quantities of documents like emails and user files for relevant information that a review team would slog through using brute force, and

2. Identify critical connections the review team could miss.

Once digested, AI can assist in interview outline preparation, interview documentation, and report preparation. In each of these areas, AI may be an imperfect tool, and compliance personnel are best suited to not rely exclusively on the work of AI in these areas.

AI in compliance self-assessment

The compliance function can use AI to evaluate its own performance and identify areas for continuous improvement. For example, AI could have a role in assessing policy efficacy and identifying lessons learned or not learned.

Policy efficacy

The quantity and nature of inquiries to guidance resources (like the chatbot discussed above) or

reports to hotlines may signal an issue with policy efficacy or a need for greater policy socialization. A compliance staffer may lack the time to conduct such an analysis or miss connections across large volumes of data. AI can quickly analyze these inquiries and reports for such issues, easing the burden on the compliance function.

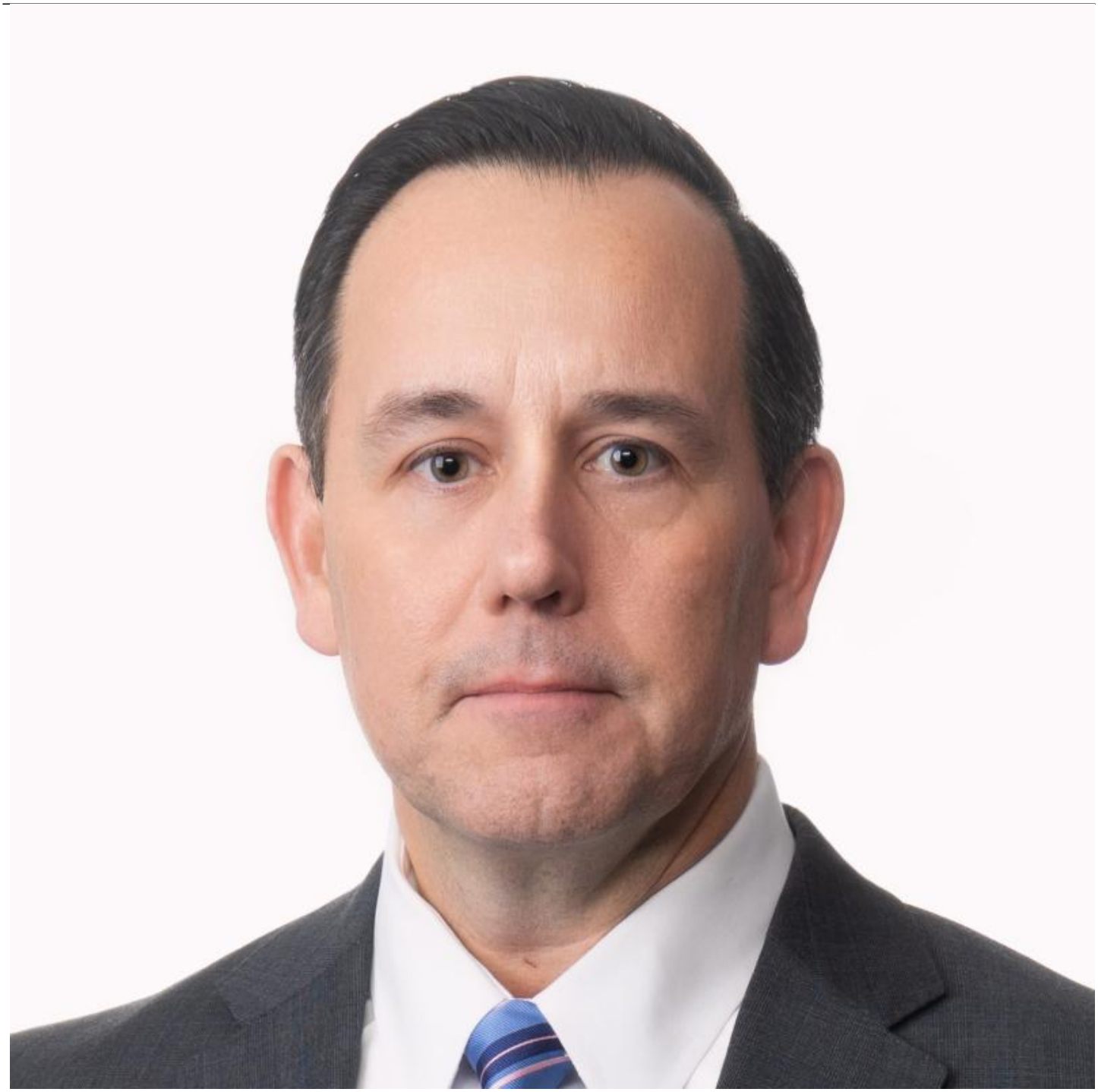
Lessons learned

The reduction (or not) in recurrence of types of misconduct may signal company personnel have learned lessons (or not) from how the company addressed the past misconduct. The ECCP update includes additional discussion of learning from past misconduct (both at the company and, newly, in the company's industry). Divining lessons learned (or not) across history has been a perennial challenge for compliance functions with limited resources. AI can process a company's investigation history to assist the compliance function's determination of whether company personnel are learning from past misconduct and its resolution. Further, AI can process public information to identify industry-specific compliance issues about which a company should be aware.

Use the guidance as a lighthouse to avoid the rocky shores of malign use

The 2024 ECCP update is a lighthouse for companies navigating the uncertain waters of the rapidly evolving world of AI and disruptive technologies. It warns of the perils — the rocks of malign use — and the DOJ's focus on those perils. And it guides to relative safety — a harbor calmed by the breakwater of risk awareness and mitigation. Companies with exposure to AI and disruptive technologies are well served by understanding the ECCP update and the recommendations embedded in it.

Daniel Christmas



Chief Compliance Officer

Corning Incorporated

As Chief Compliance Officer, Daniel Christmas is responsible for leading Corning’s global compliance organization, managing investigations, compliance policies, and processes to ensure Corning’s code of conduct and values are brought to life worldwide and that Corning's compliance program is in line with regulator expectations. He is also responsible for advising internal clients on a variety of compliance and regulatory areas, including government investigations, data privacy, government contracts, and export controls and sanctions.

Kathryn M. Rattigan

Partner

Robinson+Cole

Kathryn Rattigan is a partner in Robinson+Cole’s Data Privacy + Cybersecurity and Artificial Intelligence teams advising clients on data privacy and security, cybersecurity, and compliance with related state and federal laws. She assists clients in assessing risks related to technology and software contracts, as well as with compliance-related issues with outsourcing and vendor management. krattigan@rc.com

David E. Carney

Partner

Robinson+Cole

David Carney is a partner on Robinson+Cole’s government enforcement and white-collar defense team and the internal investigations and corporate compliance team with extensive experience in government enforcement, internal investigations, civil litigation, and corporate compliance programs. Carney uses his 25 years of experience to guide corporate and individual clients to effective and efficient resolutions of complex matters while minimizing business and personal disruptions. dcarney@rc.com