

Using Compliance-Based Criminal Charges to Prosecute Companies for AI Crimes

By Leo Tsao, Robert Luskin and Corinne Lammers

February 13, 2025

Artificial intelligence (AI) continues to dominate the headlines as a transformational tool that promises to change our lives in fundamental ways. Companies in particular are increasingly including AI tools as part of their strategic plans to make their business operations more productive, efficient, and ultimately, profitable. A subset of those companies also are incorporating AI into customer-facing solutions, and as investments continue to flow into AI, the pace of adoption will only increase.

At this relatively early stage, however, it is not readily clear what threats AI may pose to society, including potential violations of criminal laws. As we explained in an earlier article, because an AI system has no mind with which to form a criminal intent, where decisions made by AI systems lead companies to violate the law, prosecutors will likely face substantial hurdles under existing laws to prosecute corporations for crimes caused by faulty AI decision-making. But that does not mean that prosecutors are powerless to charge corporations with AI-based crimes. A corporation may still be charged if it fails to take adequate steps to test and control the AI system to prevent the violations from happening in the first place. Companies that fail to do so could face charges for compliance-based crimes. Notably, these compliance-based crimes should not be seen as second-class citizens, as evidenced by recent billion-dollar corporate resolutions brought by the Department of Justice



Photo: Production Perig/stock.adobe.com

(DOJ) charging what are essentially compliance-based failures, such as failing to implement an effective system of internal accounting controls or failing to adopt an adequate anti-money laundering program. As a general operating principle, companies should assume that their compliance programs will, at some point, become the focus of a criminal investigation. For companies adopting AI solutions for their business operations, that principle takes on heightened importance.

It is thus not surprising that the DOJ's Criminal Division recently issued new compliance guidance focused on what companies should do to mitigate AI and other new technologies from becoming a new source of risk. By doing so, the DOJ has put companies on fair notice of its expectations on how companies can responsibly adopt AI tools. Companies that take the

necessary steps may benefit from a de facto “compliance defense,” but those companies that fail to heed this guidance expose themselves to the risk of prosecution.

The DOJ’s Evaluation of Corporate Compliance Programs

On Sept. 23, 2024, the DOJ issued the latest version of the Evaluation of Corporate Compliance Programs (ECCP) with substantial changes focused specifically on what companies should consider when adopting new technologies, with a particular focus on AI. The new ECCP guidance makes clear that companies adopting AI as part of their business operations should build a program to monitor and test the AI system’s trustworthiness, reliability, and use in compliance with the company’s code of conduct and legal requirements. This is done through conducting a risk assessment regarding the intended use of AI and implementing appropriate controls to mitigate the identified risks; taking steps to mitigate the risk of bad actors deliberately or recklessly misusing the AI; and monitoring and testing the use of AI, including a baseline of human decision-making to assess the quality of the AI system. Because the DOJ’s guidance is light on details on what constitutes an “effective” AI compliance program, companies will need to decide for themselves what steps are necessary to meet DOJ’s expectations. It is important, however, that companies take steps now to understand these expectations because, while meeting these requirements should not be construed as a safe harbor from prosecution, demonstrating to the DOJ that the company has done so should be strong evidence that criminal charges are not appropriate.

Conducting an AI Risk Assessment

As an initial step, companies intending to use AI in their internal business operations or as part of their market offering to customers need to assess the risks related to their use of AI. The complexity of the risk assessment will

necessarily be fact-intensive, and depend upon factors including, for example, how the company intends to utilize AI and to what extent human actors will remain involved in decision-making. The assessment should also include an analysis of how the AI system may cause violations of the company’s own policies or applicable laws, including criminal laws. The assessment should include a review of the company’s existing compliance program, including:

- Governance around the use of AI;
- Controls currently in place to mitigate the risk of potential negative or unintended consequences resulting from AI use; and
- Controls currently in place to mitigate the potential for deliberate or reckless AI misuse.

After completion of the assessment, companies should develop additional risk mitigation measures or controls as needed. Given the fast pace of innovation in AI technologies, companies should develop a process for periodically refreshing the assessment by reviewing and managing new internal and external risks. By incorporating management of AI risk into their broader enterprise risk management (ERM) strategy, companies can standardize the process and facilitate ongoing risk surveillance.

Preventing Deliberate Misuse of the AI System

After completing the AI risk assessment, the company should develop policies, procedures, and internal controls as needed to further manage the identified residual risks. The first step is adopting policies and procedures that reflect and address the spectrum of risks created by the company’s specific use of AI. These new policies and procedures should be carefully crafted to address the potential that employees can misuse AI either to fool or bypass the company’s own or another company’s internal controls or facilitate misconduct within the company’s business model.

For example, the company’s employees could utilize AI tools to create fake documentation allowing them to bypass internal controls. A

company could misuse AI in its own business model through, for example, discrimination through AI-driven pricing models or by using AI-driven pricing algorithms to collude with competitors or improperly manipulate pricing. A well-designed compliance program should utilize policies and procedures to give both content and effect to ethical norms and to mitigate the risks identified by the company's risk assessment, especially in an area as dynamic and rapidly evolving as AI.

These AI-focused policies and procedures should be supported by internal controls designed to prevent and detect improper AI use, including that the technology is used only for permitted purposes. These internal controls may include limitations on access to AI systems based on employee roles, use of monitoring tools to help detect anomalies, and requirements to track and store AI output or decisions. All relevant employees, including those using or relying on AI as part of their job functions, should be trained on the permissible uses of AI and the company's relevant policies and procedures.

Ensuring Adequate Human Involvement and Oversight

After implementation of relevant policies and procedures, the DOJ expects companies to conduct monitoring and testing to evaluate whether the AI systems and related internal controls are functioning as intended and consistent with the company's code of conduct and related policies. A critical component of a company's monitoring and testing activities is adequate human oversight of AI systems. Internal controls should be in place to support monitoring by compliance or other appropriate personnel to verify the AI system's trustworthiness, reliability, and use in compliance with applicable law. These controls—combined with the company's monitoring and testing efforts—should also enable a company to detect if an AI system is no longer working as intended and is creating outcomes that are

inconsistent with the company's values. If such issues are found, the company needs to address and modify the AI application or its use and then to continue monitoring and testing to verify that the improper outcome has been corrected.

Further, the DOJ will specifically inquire about the level of human decision-making involved in the execution and assessment of any AI use. Companies will not be able to hide behind the "black box" of how an AI system is making decisions for the company. The DOJ will look to understand how and why AI systems are making certain decisions, and companies should consider how they would explain and defend their AI usage to regulators. More specifically, companies should be prepared to explain how appropriate compliance or other dedicated personnel assess and monitor the AI systems to get comfort that they are operating as intended. Personnel responsible for AI oversight should be granted sufficient autonomy and resources in order to do their job effectively. This will also involve having sufficient access to relevant sources of data to allow for timely and effective monitoring and testing of policies, controls, and transactions.

What Are the Takeaways?

Companies adopting AI solutions as part of their business operations need to consider implementing effective AI compliance before they begin using AI. If prosecutors cannot charge corporations with intent-based crimes for violations caused by AI systems, they will most likely turn to compliance-based criminal charges to hold companies accountable for violations of the law. Proactively adopting an effective compliance program to address AI risks may serve as a de facto "compliance defense" allowing companies to avoid criminal, compliance-based charges for AI-based crimes.

The DOJ has raised the bar for corporate compliance programs with its recent AI-focused ECCP enhancements. Companies seeking to meet the DOJ's expectations should consider the following:

- Companies seeking to implement AI solutions to supplement or replace human decision-making should—at the outset—conduct an assessment to consider the risks presented by the AI systems in use within their organization. Companies should evaluate, for all business-related functions that are impacted by AI, the probability that a particular risk (e.g., the AI system will allow an illegal transaction to proceed) will materialize and the resulting impact. Once the risks have been identified and assessed, companies can consider what controls are already in place that mitigate the risk and evaluate the residual risk in light of their risk tolerance.

- Following this assessment, companies should ensure that an adequate governance system exists to manage and assess the AI system. The responsible team should look to establish or enhance a compliance framework that implements any additional policies, procedures and controls that effectively mitigates the risks posed by AI, including the possible intentional misuse of AI.

- On the back end, once a company has implemented an AI system, they will need to institute appropriate mechanisms, including adequate human oversight, for testing and monitoring to verify that the system is working as intended. This may include running a parallel program to verify the accuracy of and any unintended outputs (e.g., bias) from an AI-driven process.

- As monitoring and testing is conducted, the results should form the basis of a feedback loop that drives further refinement of the AI system. Supported by testing results, companies should periodically evaluate their use of AI—and other new technology—to identify emerging risks and implement mitigation strategies, including ongoing monitoring of

reliability and how human judgment is used to assess appropriateness of AI-driven activities.

- Companies should provide their compliance or other dedicated teams with the necessary systems, technology, and data, and consider whether it is reasonably proportionate to the resources used for supporting the use of AI for business operations.

Paul Hastings of counsel Josh Christensen and associate Andrew Sterritt contributed to preparation of this article.

Leo Tsao is a partner in the investigations & white-collar defense and fintech & payments practices at Paul Hastings based in the firm's Washington, D.C., office. His practice focuses on internal corporate investigations, defense of criminal and regulatory enforcement actions, and compliance counseling. Before joining the firm, Tsao served for more than 15 years as a white collar prosecutor with the U.S. Department of Justice (DOJ), where he led or supervised many of the DOJ's most significant corporate criminal cases involving foreign corruption, money laundering and economic sanctions.

Robert Luskin is a partner in the investigations and white-collar defense practice at the firm based in the firm's Washington, D.C., office. He concentrates his practice on complex criminal litigation at both the trial court and appellate level. Beginning his career in government service, and having later transitioned into private practice, Luskin has represented clients in virtually every high-profile matter in Washington, D.C., over the last three decades, including members of Congress, senior White House staff, and federal judges.

Corinne Lammers is the chair of the compliance & regulatory counseling practice at the firm, based in the firm's Washington, D.C., office. Her practice focuses on compliance counseling and strategy, including compliance program development and enhancement, risk assessments, and testing and monitoring.