The US Government Is Using AI To Detect Potential Wrongdoing, and Companies Should Too

This article was published in the March 2024 issue of *Insights*.

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Anita B. Bandy
Partner / Washington, D.C.
202.371.7570
anita.bandy@skadden.com

Emily A. Reitmeier
Partner / Palo Alto
650.470.4551
emily.reitmeier@skadden.com

Mayra C. Suárez
Counsel / Washington, D.C.
202.371.7364
mayra.suarez@skadden.com

Shirley Diaz
Associate / Washington, D.C.
202.371.7362
shirley.diaz@skadden.com

Key Points

– The U.S. government's increasing use of AI and other data analytics tools to detect wrongdoing has made it essential that companies adopt similar technology for themselves.

– Data tools are now available from a variety of vendors to help flag high-risk business activities and monitor compliance to spot possible violations.

– AI technology can also be used after a government investigation is launched to quickly assess a company's potential exposure, and to sift through documents to identify those that may be relevant.

– While the technology has enormous potential, companies need to be attuned to the limitations and ensure that AI is used with close human supervision.

The use of data analytics to identify potential violations of law has become increasingly sophisticated. Agencies like the Securities and Exchange Commission (SEC) have led the charge, employing risk-based data tools to scrutinize corporate financial reports and trades. The advent of large language models like ChatGPT will only increase the ability of regulators to sift through sprawling data sets to identify potential misconduct.

With such tools at the government's disposal, companies should also take a data-driven approach to compliance and consider adopting some of these advanced technologies for that purpose.

The Government's Use of Data Analytics

For over a decade, the SEC has harnessed data analytics in oversight and enforcement. For example, the agency leverages artificial intelligence (AI) to detect trends in the thousands of tips, complaints and referrals it receives. The SEC has also used data analytics for years to uncover potential insider trading and inaccuracies in financial reporting.

The US Government Is Using AI To Detect Potential Wrongdoing, and Companies Should Too

Notably, in 2018, the SEC launched the Earnings Per Share (EPS) initiative, which uses risk-based data analytics to uncover potential accounting and disclosure violations caused by earnings management and other improper practices.

The EPS initiative alone has resulted in at least six enforcement actions to date, most of which have involved fraud charges and significant penalties against the relevant companies and individuals.

The Department of Justice (DOJ) also leverages data analytics for investigations. For example, the Criminal Division recently touted the use of data to identify potential wrongdoing involving foreign corruption. Likewise, the Antitrust Division's Procurement Collusion Strike Force — a joint law enforcement effort to address antitrust crimes — established a project to develop data tools for identifying suspicious bid patterns three years ago. (See "The Meteoric Rise of Generative AI Has Regulators Gearing Up To Preserve Competition.")

As Assistant Attorney General Nicole Argentieri noted in November 2023, given the success of data analytics, the DOJ is "going to double down on these efforts to allow [it] to identify additional misconduct that may otherwise have gone undetected." The DOJ expects companies will similarly "up[] their game" with respect to data analytics, she added.

Assistant Attorney General Argentieri's comments and the actions of the SEC and DOJ send a clear message to corporations: The tools and methodologies used by regulators should be reflected in corporate compliance programs.

The importance of adopting these tools has only been heightened by the emphasis the DOJ has placed since 2022 on the role of voluntary self-disclosure of possible corporate misconduct. The new technology can both help to uncover possible wrongdoing before the government does, allowing self-disclosure, and demonstrate a company's commitment to rigorous compliance. In both instances, the company can earn credit if the DOJ seeks to impose penalties.

In-House Compliance: The Rise of SupTech

Supervisory technology (SupTech) — machine-learning technology that lessens the burden of complying with or supervising compliance with regulatory requirements — is revolutionizing compliance.

The capacity to manage and analyze data is a cornerstone of effective compliance programs. One need look no further than the DOJ Criminal Division's Evaluation of Corporate Compliance Programs, which asks prosecutors to assess whether compliance programs are "based upon continuous access to operational data and information across functions."

In the context of settlement negotiations, the government will likely credit companies using data analytics. For example, in a recent settlement involving potential violations of the Foreign Corrupt Practices Act (FCPA), the DOJ viewed positively the company's use of data analytics for monitoring and measuring the effectiveness of its compliance program, Assistant Attorney General Argentieri has stated.

Potential Strategic Initiatives for Compliance

SupTech is useful not just for finding potential wrongdoing; it is also going to be part of what regulators expect to find in a robust compliance program. There are many vendors developing these types of tools, which can be implemented using a company's existing data sources.

Strategies that companies might consider adopting include:

- **Predictive compliance analytics.** Developing predictive models to anticipate compliance risks enables companies to address potential issues proactively. In the event of a government investigation, these models serve as evidence of a diligent, data-informed approach to compliance, potentially mitigating penalties. These tools can continuously assess and update the risk profiles of various corporate activities — from foreign dealings to procurement processes — and help identify patterns like those the DOJ's Procurement Collusion Strike Force might look for. Developing such tools can enable preemptive action.

- **Real-time compliance dashboards.** By employing AI-driven dashboards for continuous compliance monitoring, companies can swiftly identify and rectify potential breaches. This capability also showcases an ongoing, real-time commitment to compliance integrity.

- **AI-enhanced whistleblower systems.** Advanced platforms to receive whistleblower complaints that prioritize and anonymize reports not only encourage a culture of integrity but also enable early detection and self-reporting of issues to regulators, which may result in significant cooperation credit in investigations.

- **AI-assisted management of regulatory changes.** An AI system dedicated to tracking and analyzing regulatory changes ensures that companies remain ahead of compliance requirements. Demonstrating to regulators that a company has a dynamic, responsive compliance program can be advantageous during investigations.

Navigating Investigations With Tech-Driven Compliance

In the event of a government investigation, companies can use AI tools to better determine early on whether there is an issue. Such tools can process vast amounts of data at speeds and depths impossible for human investigators to perform. For instance, the technology can sift through years of transactional data to identify

The US Government Is Using AI To Detect Potential Wrongdoing, and Companies Should Too

anomalies that may indicate irregular payments, such as bribes or unauthorized disbursements.

By learning from historical data, these systems can flag transactions that deviate from established patterns within hours, not weeks.

AI tools can also analyze vast repositories of emails, documents and text messages to predict their relevance to an ongoing investigation. Natural language processing (NLP) techniques also enable AI to understand the context of communications, filter out irrelevant information and highlight materials that could indicate compliance breaches.

This targeted approach allows companies to efficiently allocate resources to review and analyze the most pertinent data and get preliminary answers to threshold questions.

Limitations

Despite the clear benefits, integrating new technologies with existing systems presents significant challenges, including compatibility issues and the need for substantial training and change management. Companies must also ensure that the technologies they deploy comply with applicable laws, including data privacy laws.

Deputy Attorney General Lisa Monaco also commented in March 2024 that, given the prolific use of AI, "prosecutors will [now] assess a company's ability to manage AI-related risks as part of its overall compliance efforts." The DOJ is still forming its policies on AI and will begin convening meetings with stakeholders in an initiative it calls "Justice AI." Further, DOJ prosecutors may seek stiffer penalties for misconduct involving AI technology, she said in another speech.

There are also risks to models made by humans. For example, the underlying code may become stale, or a typo in the code could set an unwanted parameter or limit. As a result, human oversight and ownership are still critical. Additionally, one can expect regulators to scrutinize the algorithm or model of any compliance program in case of an investigation.

A Proactive Stance on Compliance

As sophisticated technology-enabled regulatory scrutiny intensifies, the role of technology in compliance has transitioned from a supplementary tool to a central pillar of corporate governance.

By integrating advanced technology solutions, companies not only enhance their ability to adhere to regulations but also position themselves favorably in the event of regulatory investigations. Through early detection, self-reporting and transparent demonstration of compliance efforts, corporations can navigate the complexities of investigations more effectively, potentially securing cooperation credit and influencing regulatory outcomes.