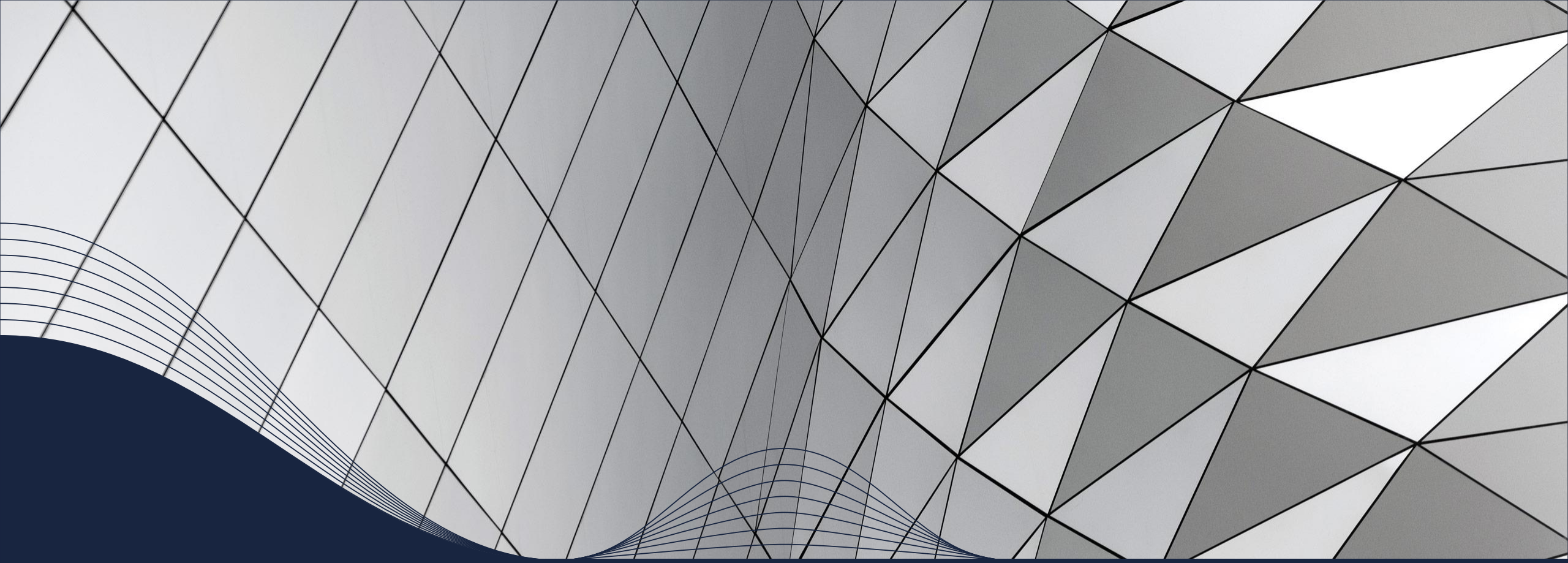


Artificial Intelligence (AI) Under Investigation: Enforcement Risks and Compliance Challenges

May 6, 2025

DLA PIPER

Panelists

Jonathan Haray
Partner
White Collar, Investigations and Government Enforcement

Jonathan Haray represents corporations and individuals in government investigations, securities and regulatory enforcement matters, and white-collar litigation. Recognized by Chambers USA and the National Law Journal as being a leading white-collar government investigations and criminal defense lawyer, Jonathan advises corporate clients on sensitive matters involving government regulators and law enforcement agencies, as well as in commercial disputes and internal investigations.

Aurélie Ercoli
Partner
White Collar, Investigations and Government Enforcement

Aurélie is a French American lawyer advising global companies on US enforcement risks and related enforcement actions. As a native French speaker qualified in France and in the US, Aurélie helps clients navigate enforcement risks across these two jurisdictions, complex fraud issues and AI-related risks.

Ashley Carr
Partner and AI Counseling Lead
AI & Data Analytics

Ashley Carr is a seasoned products liability and commercial litigator with specialized and deep experience in risk prevention and disputes involving life sciences, artificial intelligence, and software. She represents healthcare, life science, pharmaceutical, medical device, and technology companies in a variety of litigation matters, including complex commercial litigation and product liability cases. She also regularly counsels clients on a wide range of issues, including risk management and state and federal regulatory matters.

Darryl Tarver
Of Counsel
White Collar, Investigations and Government Enforcement

Darryl Tarver is a seasoned trial lawyer and versatile litigator. Drawing on his prior experience as a federal prosecutor, Darryl approaches disputes, government inquiries, investigations and other engagements with poise and preparation. In private practice, Darryl has represented global product manufacturers, retailers and insurance companies in civil litigation in state and federal courts. He has also handled internal corporate investigations in high-stakes scenarios.

Introduction

AI is transforming industries

AI is revolutionizing sectors such as healthcare, finance, transportation, and more, driving innovation and efficiency.

Potential risks of AI misuse

Lack of oversight, biased algorithms, and unintended consequences can lead to significant harm if AI is not developed and used responsibly.

Need for AI governance

Effective AI governance and compliance programs are critical to mitigate the enforcement risks associated with the use of AI technologies.

As AI continues to reshape industries, it is crucial to address the potential risks and establish robust governance frameworks to ensure the responsible development and deployment of these transformative technologies.

Key US government pronouncements on AI

April 2023. Joint-statement of four US government agencies pledging to investigate AI development and use.

February 2024. “Justice AI” initiative.

April 2024. Six additional government agencies join the pledge to investigate AI development and use.

September 2024. The Department of Justice (DOJ) amends its guidance on Evaluation of Corporate Compliance Program (ECCP) to incorporate AI-related risks.

January 2025. Executive Order Removing Barriers to American Leadership in AI.

April 2025. White House’s revised policies on Federal Agency Use of AI and Federal Procurement.

Enforcement trends overview

- **No uniform legislation in the US regulating the development and use of AI**
  - Private plaintiffs and US law enforcement authorities are relying on existing statutes to fight against the harm caused by the misuse of AI
- **AI-related corporate enforcement actions rely on misrepresentations made about the use of and/or the capabilities of AI**
  - No AI-based criminal statutes
  - Theories of liability vary depending on who was impacted by the misrepresentation
  - Three major categories of impacted parties: investors, consumers, and the US government

Enforcement to combat harm caused to the US government

Leading government agencies and existing statutes

- **Leading law enforcement authorities include:**
  - DOJ Fraud sections in both its Criminal and Civil Divisions
  - Office of Inspector General within each federal agency
- **Key existing statutes include the False Claims Act (FCA) and criminal fraud offenses**
  - DOJ has expressed an ongoing commitment to aggressive enforcement to combat fraud pertaining to electronic health records
  - DOJ's increased reliance on data analytics to identify and pursue potential fraud cases
  - Recent White House Guidance for AI acquisition and use in government may serve as roadmap for government contractors on how the US government expects its contractors to use and deploy AI

Enforcement to combat harm caused to the US government

Relevant enforcement actions

US v NextGen Healthcare (2023)

US v Alere Inc. (2021)

US v Practice Fusion (2020)

US v Greenway Health, LLC (2019)

US v eClinicalWorks, LLC (2017)

Enforcement to combat harm caused to consumers

Leading government agencies and existing statutes

- Leading federal law enforcement agencies include the DOJ and the Federal Trade Commission (FTC)
- April 2023 and April 2024 Joint Statements:
  - Signal new criminal investigations into AI-related conduct affecting consumers
  - Highlight that regulation of AI falls squarely within: (1) the ambit of existing federal laws; and (2) the agencies' collective authority to enforce civil rights, non-discrimination, fair competition, and consumer protection
- September 2024 FTC announcement regarding "Operation AI Comply"
- Agencies are leveraging federal consumer protection laws and antitrust laws

Enforcement to combat harm caused to consumers

Leading government agencies and existing statutes

- As the new administration rolls back the prior administration's regulatory framework on AI, states Attorneys General (AGs) are filling in the void by:
  - Passing AI legislation, which often includes states AGs enforcement authority
    - Colorado AI Act
    - California AI Transparency Act
  - Issuing guidance on how state AGs intend to leverage existing state laws to regulate, investigate and enforce against artificial intelligence
    - California, Massachusetts, New Jersey, Oregon, and Texas advisories and guidance
    - New York Department of Financial Services guidance on use of AI

Enforcement to combat harm caused to consumers

Relevant enforcement actions

In re Workado, LLC (April 2025)

In re DoNotPay, Inc. (February 2025)

US v Real Page, Inc. (August 2024)

Enforcement to combat harm caused to investors

Leading government agencies and existing statutes

- The Securities and Exchange Commission (SEC) and the DOJ are the two leading government agencies conducting enforcement over AI-related misrepresentations to investors
- Both agencies are leveraging existing statutes to do so
  - March 2025 SEC Roundtable on AI reiterated the agency's intent to rely on existing legal frameworks to pursue AI-related misconduct
  - Key existing statutes include the Securities Exchange Act and Title 18, US Code offenses for securities, mail and wire fraud

Enforcement to combat harm caused to investors

Relevant enforcement actions

In re Delphia and In re Global Predictions (2024)

In re Presto Automation (2025)

US v Saniger and *SEC v Saniger* (2025)

DOJ's renewed expectations on AI-related risks

Identifying and addressing AI-related risks

- **Corporate compliance programs expected to address "emerging risks," which include AI**
  - Emerging risks defined as those associated with new and emerging technology used to conduct business
  - Corporate compliance programs expected to proactively assess and address these risks
- **AI-related risks include:**
  - Lack of sufficient/sophisticated technology;
  - Technology failure;
  - Lack of sufficient policies and procedures;
  - Data privacy and security concerns; and
  - Ethical considerations.

DOJ's renewed expectations on AI-related risks

Incorporating AI-related risks into corporate compliance programs

- **DOJ expects corporate compliance programs to:**
  - Assess the potential impact of new technologies, such as AI, on its ability to comply with criminal laws
  - Mitigate the negative or unintended consequences from the use of emerging technologies in business and in compliance programs
  - Mitigate deliberate or reckless misuse of technologies including by company insiders
  - Maintain controls to ensure that technology is trustworthy, reliable, and used in compliance with applicable laws and the company's code of conduct
  - Monitor and enforce accountability over the use of emerging technologies to quickly identify any non-compliance and ensure it is only used for its intended purposes
  - Train employees on the use of emerging technologies

Common elements of an AI governance program

Good AI Governance Addresses Enterprise Risks

Regulatory uncertainty	Product liability risk	Risk of fraud	Limited AI fluency and unharmonized terminology
Fragmented internal safeguards	Intellectual property and confidentiality	AI system quality concerns	AI privacy/ security risk
Lack of accuracy/bias	Insufficient contractual protections	Unclear procurement standards	Reputational risk

Common elements of an AI governance program

Certain key features can set an AI governance program up for success

Flexible But Effective Controls – best practice controls are tailored to level of risk, are supportive and enable innovation, and are top-down with increasing specificity from enterprise value statement and policy to unit/department procedures

Targeted Testing – testing protocols should be tailored to use case needs, be benchmarked to industry standards, and be adaptive and evolutionary to meet changing regulatory and industry standards

Routine Monitoring – clear reporting requirements and structures for monitoring AI higher-risk use after deployment should be in place to ensure continued compliance with evolving regulations and legal landscape

AI Training – training is appropriate to level or role in oversight, business, and legal fields

- Goal is issue-spotting fit to level, ability to risk stratify, and knowing when to escalate

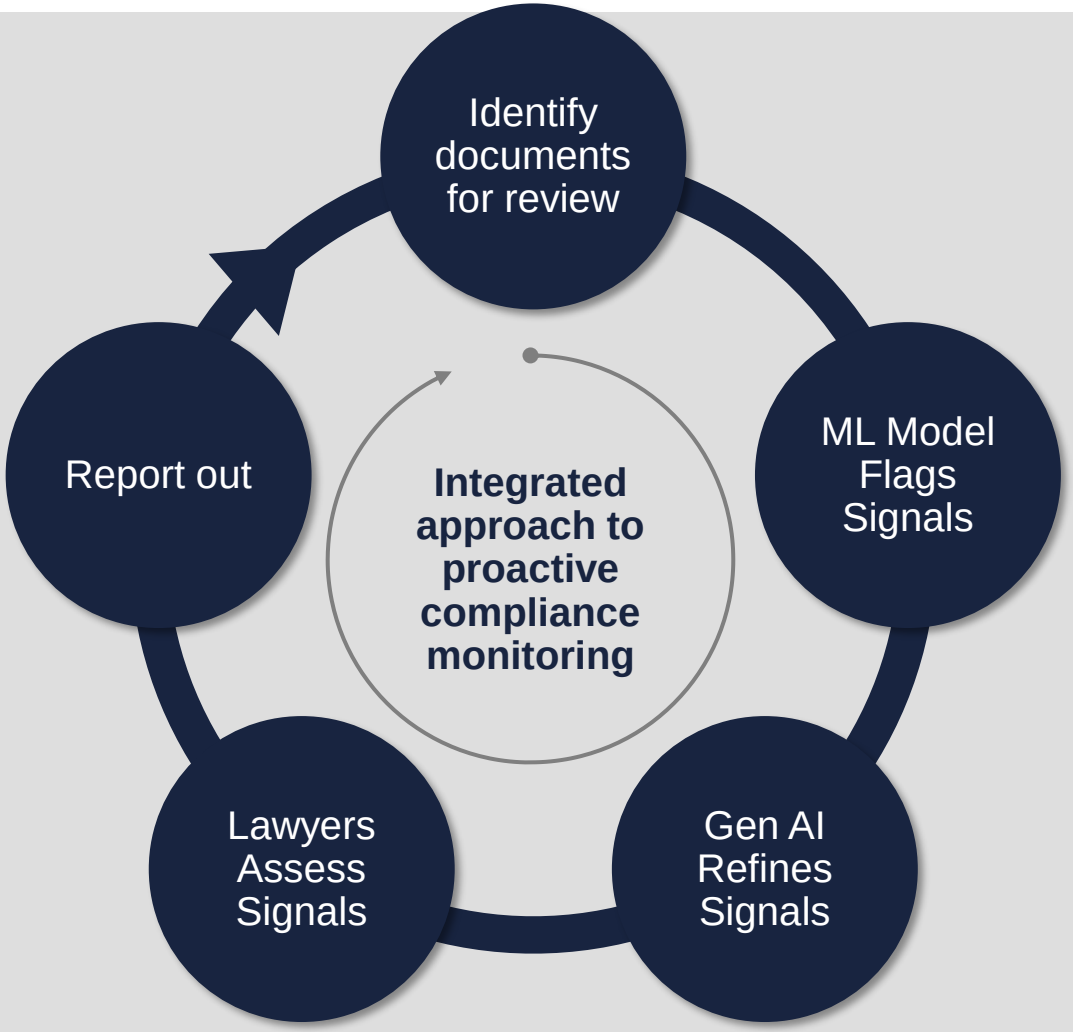
DOJ’s renewed expectations on AI-enabled compliance

AI for risks mitigation and compliance

- Under the revised ECCP, companies are expected to:
  - Enable the Compliance function to timely access all relevant data sources
  - Leverage data analytics tools to create efficiencies in compliance operations and test the effectiveness of the company’s compliance program
  - Measure the accuracy, precision, and recall of data analytics models they are using
  - Ensure there is no imbalance between the resources and technology deployed to capture market opportunities and those deployed to detect and mitigate risks

DOJ's renewed expectations on AI-enabled compliance

Examples of AI-enabled proactive compliance services: transforming unstructured data into actionable insights



Case study

Cost effective messaging data monitoring

Our team conducted proactive compliance monitoring for a Fortune 100 client to enhance corporate controls for preventing statutory noncompliance and illuminate any emerging risks within messaging data. While this client has a robust ethics and compliance program, an inability to monitor messaging data cost-effectively and at scale presented a critical compliance gap.

Our solution addresses both barriers.

Additional Resources

For more information about our AI or White Collar, Investigations and Government Enforcement solutions, please visit these links:

- White Collar and Corporate Crime
- Artificial Intelligence and Data Analytics
  - AI Legislation and AI Legal News
- AI Disputes Landscape

Thank you