From AI Principles to Proof

What DOJ Scrutiny Means for Corporate Governance

By Tom Hagy featuring Adria Perez

Editor's Note: *This article is adapted from a recent episode of* The Emerging Litigation Podcast, *featuring Adria Perez, a partner in Reed Smith's Global Regulatory Enforcement Group. For clarity and length, the conversation has been edited and condensed.*

Federal regulators are no longer satisfied with broad statements about "responsible AI." They want proof—documentation, controls, and real-world examples showing how companies actually use artificial intelligence.

That shift was the focus of a recent episode of *The Emerging Litigation Podcast*, where I spoke with **Adria Perez**, a partner in Reed Smith's Global Regulatory Enforcement Group and a former member of the Volkswagen AG Independent Compliance Monitor and Auditor team. Our conversation centered on the Department of Justice's newly announced **AI Litigation Task Force** and what it signals for in-house counsel, compliance teams, and corporate boards.

What struck me most was how far this conversation has moved beyond theory. The DOJ isn't asking whether companies *believe* in responsible AI. It's asking whether they can **demonstrate oversight**, explain their controls, and show how their AI use holds up under scrutiny—whether in compliance reviews, internal investigations, or whistleblower complaints.

DOJ Is No Stranger to AI

One misconception is that regulators are somehow behind the curve on AI. As Adria explained, that simply isn't true. The federal government has been using AI for years, including within the DOJ itself. Agencies already rely on AI tools to analyze financial records, travel data, communications, and other large datasets—often in ways that far exceed what companies imagine. That reality matters because it shapes enforcement expectations. When prosecutors review a company's compliance program, they're not evaluating AI in the abstract.

> **They are now looking at how the company uses AI," Adria said. "Do you have the right controls to mitigate bias, to make sure the AI tool is giving you something that's truthful and verifiable?"**

Under updates to the DOJ's **Evaluation of Corporate Compliance Programs**, those questions are now explicit. Companies should assume that AI usage—especially in compliance, investigations, and decision-making—will be part of any serious regulatory inquiry.

Federal–State Tension Creates Real Risk

We also spent time discussing the broader policy backdrop. The AI Litigation Task Force reflects a push toward a single national framework, particularly as states continue to adopt their own AI laws. That tension creates uncertainty for companies trying to assess risk.

Adria compared the moment to earlier ESG enforcement dynamics, when companies struggled to predict whether federal or state authorities would lead. The lesson then—and now—is that uncertainty doesn't reduce risk. It shifts it.

For most companies, state exposure still matters. If you do business in California, for example, you can't ignore how AI is regulated there, regardless of federal posture. The practical approach is the same one compliance teams have always taken: identify where your highest risks are and allocate resources accordingly.

Whistleblowers and Synthetic Evidence

One of the most sobering parts of our conversation involved whistleblowers and internal investigations. Incentives for whistleblowing have expanded, and AI has dramatically lowered the barrier to creating evidence that looks real—but isn't.

> **We have to change our mindsets. You used to be able to look at a photo and tell right away if it was manipulated," Adria said. "Now it's incredibly difficult to know whether something is AI-generated or not."**

Images, videos, and chat transcripts can now be fabricated with a level of sophistication that makes casual verification unreliable. Adria described matters where companies received AI-generated materials that initially appeared authentic, forcing legal teams to slow down and validate before acting.

That validation step is now essential. Companies can't assume that every image or document they receive is genuine. Due diligence increasingly includes verifying the evidence itself, often with the help of IT teams and forensic consultants who can analyze metadata and provenance.

The takeaway for me was simple: AI doesn't just change how misconduct happens. It changes how investigations must be conducted.

Governance Starts with Protocols

When I asked Adria what DOJ would ideally want to see from a company, her answer was consistent and practical: **clear protocols**.

A defensible AI governance framework documents when AI tools may be used—and when they may not. It distinguishes between tasks suited for generative AI and those that still require human judgment, such as privilege review. It identifies which tools are appropriate for specific functions and explains how bias and false positives are mitigated.

"AI is a tool—it can be used for you or against you, and the government understands that," Adria told me.

At Reed Smith, for example, AI is used for tasks like summarization, chronologies, and document analysis, but not for privilege determinations. Those choices are written into protocols, supported by training, and reinforced through internal audits.

That kind of documentation matters because it shows regulators that AI use wasn't ad hoc. It was deliberate.

AI in Investigations: Faster and Smarter

AI's value becomes especially clear in internal investigations. Adria shared examples of using AI tools to identify who first learned of misconduct, summarize years of emails and Teams chats, and surface key documents buried in massive datasets.

Anyone who has reviewed internal communications knows how much noise there is—casual messages, workplace banter, and irrelevant chatter. AI doesn't replace human judgment, but it dramatically narrows the field, allowing lawyers to focus on what actually matters.

The efficiency gains are real, and they benefit both clients and counsel. More importantly, they make investigations more targeted and defensible.

Don’t Hide AI from the Board

One of Adria’s strongest points—and one I think many legal and compliance teams still underestimate—is the importance of talking to the board about AI. Boards are deeply interested in how AI is being used and governed. Yet legal and compliance teams often frame AI as a risk rather than a value driver. That’s a missed opportunity.

> **“Legal and compliance departments should be bragging about their use of AI to their boards,” Perez said. “This is one of those areas where you can show the value you’re bringing to the company.”**

Responsible AI use is something companies should highlight. It demonstrates oversight, efficiency, and strategic thinking. This is an area where legal and compliance functions can clearly show they are doing much more than just managing downside risk.

The Bottom Line

AI is already embedded in enforcement, investigations, and compliance expectations. Companies that hesitate out of fear risk falling behind those that adopt AI thoughtfully, document their choices, and train their people.

As Adria put it during our conversation, if you don’t use AI, the technology will run away from you.

For legal teams, the question is no longer whether to engage with AI. It’s how to do so in a way that withstands scrutiny when regulators come calling.

HB Litigation News publishes articles, podcasts, and webinars on emerging issues in litigation. It is directed by long-time legal writer and publisher Tom Hagy, founder and director of Critical Legal Content LLC, which creates content for firms and other legal services. Editor@LitigationConferences.com.