CLIENT ALERTS & INSIGHTS

Where AI Regulation Stands Today Part 2: State Attorneys General as the Primary AI Enforcers

JUNE 22, 2026

Authors: Kevin B. Frankel, Kristopher J. Chandler, Yesul ("Kristin") Lee, Juan Mata

Featured Practices: Litigation, State Attorneys General Investigations & Enforcement, Artificial Intelligence (AI)

Key Takeaways

- State attorneys general-not federal regulators-are currently leading AI enforcement, using existing laws like consumer protection, civil rights and privacy statutes to investigate and pursue companies for AI-related risks.
- Companies face immediate and multistate enforcement exposure, even without AI-specific laws. Coordinated actions by multiple AGs can increase liability, trigger simultaneous investigations and impose nationwide compliance obligations-especially in high-risk areas like healthcare, employment and consumer-facing AI tools.
- Organizations should proactively build AI governance frameworks for multistate scrutiny, including maintaining clear documentation, auditing AI systems, managing vendor risk and monitoring AG activity-rather than waiting for federal guidance to standardize requirements.

Artificial Intelligence ("AI") governance has been shaped not only by legislative activity and federal policy initiatives, but also by rapidly evolving state enforcement activities. While the question of federal preemption of state AI laws continues to develop, companies implementing AI face a more practical and immediate question-who is bringing lawsuits and enforcement actions today? The answer is becoming increasingly clear: state attorneys general ("AGs").

State AGs possess broad enforcement authority, flexible legal tools and the ability to act quickly, often coordinating with other state AGs. These characteristics allow state AGs to address concerns about companies' AI practices today.

First, state AGs' enforcement actions against AI practices are not limited to AI-specific statutes. Rather, they operate within a broad framework of generally applicable state laws that can be extended to AI-related conduct. These include: (i) Unfair and Deceptive Acts and Practices ("UDAP") statutes; (ii) state consumer protection laws; (iii) civil rights and anti-discrimination statutes; (iv) data privacy and biometric information laws; and (v) "parens patriae" authority to act on behalf of state residents. For example, the California AG has long warned that the use of AI in sectors such as healthcare and employment remains subject to existing civil rights, consumer protection and false

advertising laws, emphasizing that companies may face liability where AI systems produce discriminatory or misleading outcomes.

This framework allows state AGs to pursue enforcement actions against AI-related risks without waiting for new legislation. An AI system that produces misleading output may be challenged under UDAP statutes. If algorithmic decision-making tools result in disparate impacts, they might also be subject to anti-discrimination laws. For example, in 2024, the Texas AG investigated an AI healthcare technology company for its false, misleading and deceptive representations regarding a generative AI product, asserting a violation of the Texas Deceptive Trade Practices-Consumer Protection Act.

Second, state AGs possess significant investigatory powers, including the ability to issue civil investigative demands, subpoena documents and compel testimony. These tools enable them to initiate investigations and develop enforcement theories before formal litigation begins, often placing companies in a defensive posture early in the process.

Third, state AGs are structurally incentivized to respond to emerging risks. Many AGs are elected officials. AI-related issues-particularly those related to consumer harm, employment practices or public safety-are politically salient. This dynamic creates pressure on AGs to act proactively, even in areas where widely agreed-upon legal standards are still developing. That incentive is already translating into an aggressive enforcement posture. For example, in April 2026, the Florida AG launched a criminal investigation into an AI company to determine whether the company could bear legal responsibility for its chatbot's representations and functionality in facilitating a violent incident. More recently, in May 2026, the Pennsylvania AG sought preliminary injunctions against an AI company for falsely representing its chatbot to be a licensed psychiatrist in violation of the Pennsylvania Medical Practice Act.

Finally, state AGs have a history of leading enforcement in emerging regulatory areas. State AGs have consistently played a role in the early enforcement landscape, particularly where the impetus for regulation moved at a breakneck speed, such as in data privacy and antitrust. AI presents a similar dynamic where the technology is evolving faster than traditional legislative and regulatory processes. State AGs are inherently more primed to define the AI enforcement landscape while broader federal initiatives continue to develop.

While federal agencies possess similar tools, they are at a disadvantage when it comes to swiftly taking action compared to state AGs. Federal efforts are often constrained by supervisory and geographical jurisdictions and administrative processes. As discussed in Part 1, federal AI oversight remains fragmented. Federal authority is distributed across multiple agencies, with each operating within sector-specific mandates. While recent executive actions have emphasized coordination, they have yet to establish a unified enforcement regime capable of addressing AI risks comprehensively. By contrast, state AGs can act swiftly without being weighed down by similar bureaucratic challenges.

With state AGs as the primary enforcers, companies should be aware of enforcement through multistate coalitions. These coalitions allow multiple AGs to coordinate investigations, share information and pursue unified enforcement actions. Multistate enforcement has long been a hallmark of state AG activity in areas such as data breaches and consumer protection. The same model has been and will continue to be applied to AI-related risks. For example, on February 25, 2026,the Connecticut AG issued guidance on

The Application of Existing Laws to Artificial Intelligence to Protect Connecticut Residents, confirming that existing state laws, including anti-discrimination and consumer protection statutes, apply directly to AI systems, and mirroring Massachusetts AG Andrea Campbell's Advisory on the Application of the Commonwealth's Consumer Protection, Civil Rights, and Data Privacy Laws to Artificial Intelligence from 2025. Resulting multistate enforcements can create several distinct challenges:

- **Aggregated Exposure:** Coordinated actions can significantly increase potential liability by combining claims across jurisdictions.
- **Uniform Compliance Obligations:** Settlement agreements may require companies to adopt nationwide changes, even where legal requirements vary by state.
- **Simultaneous Investigations:** A single issue may trigger inquiries from multiple AG offices, increasing complexity and cost.

Multistate coalitions often operate independently from federal enforcement efforts, such as the bipartisan coalition of 44 state AGs that issued a coordinated letter to major AI companies. The AGs raised concerns about safety in AI systems that interact with children. Federal policy might eventually narrow certain categories of state regulation through preemption or litigation. However, in the near term, coordinated state enforcement remains a primary risk driver.

Several trends are already emerging from state AG activities that have an immediate impact on companies developing or deploying AI systems. First, compliance must be designed for multistate exposure. Considering multistate coalitions, companies should adopt governance frameworks that can withstand scrutiny across jurisdictions, rather than relying on state-specific approaches.

Second, investigations may precede clear regulatory standards. State AGs are not required to wait for formal AI-specific legislation and centralized regulatory frameworks before initiating enforcement actions, and many are already applying existing consumer protection, civil rights and privacy laws to AI-related conduct. Current enforcement attention is focused on high-impact sectors such as employment, healthcare, lending and housing, as well as on generative AI systems that produce misleading outputs or rely on opaque data practices. State AGs are also increasingly scrutinizing AI applications affecting minors, including recommendation systems, content moderation tools and data collection practices.

Third, documentation and governance are critical. In an enforcement context, the ability to demonstrate how AI systems were designed, tested and monitored-and how risks were identified and mitigated-can significantly affect outcomes.

Fourth, vendor and third-party risk must be actively managed. Many AI systems rely on external providers, but companies, not vendors, remain responsible for compliance. Contractual protections, audit rights and clear allocation of responsibilities are essential.

In light of these dynamics, companies should take the following proactive steps to address state-level enforcement risk:

- Evaluate comprehensive inventories of AI systems and their uses;
  - Implement risk-tiering frameworks to prioritize high-impact applications;
  - Establish governance structures with clear accountability for AI oversight;
  - Develop and maintain documentation supporting system design, testing and monitoring;
  - Ensure clear and accurate disclosure regarding consumer-facing AI systems; and
  - Monitor state AG activity and multistate initiatives to anticipate enforcement trends.

The goal is to establish measures that align with the broader federal expectations discussed in part one of this series, while directly addressing the realities of state-driven enforcement. AI compliance must be designed with state enforcement in mind. Companies that proactively address governance, transparency and risk management will be better positioned to navigate this environment. Those simply relying on future federal uniformity may face increased exposure during the period of regulatory transition.

Part 3 will address how companies can navigate the patchwork of state AI laws and implement scalable compliance strategies across jurisdictions.

The Benesch team stands ready to help navigate through overlapping federal and state AI laws, and to advise on regulatory updates and developments, as well as compliance strategies. If you have any questions, please contact the author or your contact point at Benesch.

Read Part 1