Reuters Legal News

Compliance in the wild west — How state AGs are using traditional legal frameworks to address AI business practices

By Ashley Taylor, Esq., Clayton Friedman, Esq., and Daniel Waltz, Esq., Troutman Pepper Locke

JULY 27, 2026

I. Cut through the noise: What state attorneys general are doing about AI

Newsfeeds are saturated with dramatic headlines about artificial intelligence ("AI") — self-driving cars, AI-generated art, hallucinated legal briefs, and predictions of technological dystopia. The constant noise can obscure a more practical reality: Artificial intelligence is, at its core, a tool. However, it does not relieve companies of their longstanding obligations to treat consumers fairly or comply with existing state law.

State AGs are increasingly scrutinizing AI products marketed as substitutes for human professionals, especially in activities typically licensed by the state.

While new AI-specific bills are emerging, state regulators need not wait for bespoke legislation to act. State Attorneys General are turning to the tools they know best — state Unfair and Deceptive Acts and Practices (UDAP) statutes and related consumer protection laws and regulations. These broadly worded laws, traditionally used to address fraudulent or misleading business practices that harm consumers, also serve as a means of creatively addressing novel concerns and emerging issues. They are now being applied to AI-driven business conduct. State AGs are also looking to antitrust, privacy, and licensing authority to achieve enforcement objectives.

II. AI does not have professional judgment

State AGs are increasingly scrutinizing AI products marketed as substitutes for human professionals, especially in activities typically licensed by the state. Some AI tools purport to function as financial advisors, lawyers, or medical providers, even though these systems cannot offer the individualized advice and professional judgment that trained humans provide.

Many licensed professionals already use AI daily. State AGs grow concerned when a product claims to fully replace those professionals entirely. When AI tools are promoted as adequate stand-ins for licensed professionals, those claims are likely to be viewed as deceptive under state UDAP law.

- **Do not imply that AI performs services that require state licensure**. Pennsylvania's Department of State recently brought a first-of-its-kind enforcement action against Character.AI, alleging that its "companion" chatbots unlawfully held themselves out as licensed medical professionals and engaged in the unlicensed practice of medicine. The complaint cites chatbot personas that purported to be psychiatrists, claimed to hold Pennsylvania medical licenses, and offered assessments and treatment recommendations to users without any actual licensure or oversight. Pennsylvania is seeking injunctive relief to stop the company from marketing or operating these bots as medical providers. A continuance has been granted, so Character.AI is set to file its Answer in response to Pennsylvania's Complaint by September 1, 2026. This case is significant because it approaches AI regulation from the perspective of the state professional licensing board — an avenue available to regulators in virtually every state — rather than through a new AI-specific law.
- **Implement safety into the design of therapy products**. State AGs are also coordinating to address risks posed by AI chatbots marketed as therapy or companion products that reach children and other vulnerable users. In December 2025, a bipartisan coalition of Attorneys General from more than 40 states and territories wrote to the legal representatives of major AI companies expressing serious concerns about "sycophantic and delusional outputs" from generative AI software, as well as deeply troubling AI interactions involving children.

The letter calls on these companies to take immediate action, including adopting stronger child safety safeguards such as age-tailoring chatbot conversations, requiring chatbots to refer users to mental health professionals or law enforcement when conversations involve self-harm, drug use, or threats of violence, and mitigating AI outputs designed to tell users only what they want to hear rather than the truth. The major AI companies have not released a public statement regarding the AG coalition's letter.

The consistent lesson from recent state AG enforcement activity is that regulators will evaluate AI through traditional legal frameworks — consumer protection, professional licensing, privacy, and advertising law.

State AGs view children's safety as one of their most significant enforcement priorities — particularly in the perceived absence of federal legislation or enforcement activity. For products used by minors, companies must be careful. They have publicly acknowledged that the most effective way to regulate AI in these early days of oversight is through enforcement actions and substantial settlements to deter undesirable business practices.

III. Regulators increasingly expect platforms to develop safeguards

AI has transformed the pace and scale of content creation. Marketers can now generate images, ad copy, and full video campaigns in a fraction of the time previously required. But this democratization has also lowered the barrier to entry for bad actors. Sophisticated-looking ads and social media posts — once the domain of well-funded operations — can now be produced cheaply by scam artists, giving consumers a misleading sense of legitimacy.

- **Build safeguards to protect consumers from AI-fueled deception**: State AGs are now specifically targeting the role of social media platforms in enabling AIdriven deception, from investment scams using deepfake impersonations and fraudulent cryptocurrency schemes to misleading AIgenerated weight-loss advertisements for GLP1 drugs that prey on consumer insecurities and obscure medical risks. The New Hampshire AG has warned residents about sophisticated investment frauds proliferating on social media platforms, while bipartisan coalitions of 35 AGs have called on social media platforms to better enforce their own policies, enhance review of highrisk ads, and curb AIgenerated scams and weightloss content that evades automated controls. In parallel, these enforcement efforts signal that regulators increasingly expect social media platforms to serve as frontline gatekeepers — policing deceptive AIenhanced ads, providing greater transparency around AI use, and, where necessary, restricting entire categories of risky advertising.
- **Prevent illegal outputs**. In January 2026, a bipartisan coalition of 35 AGs sent a joint letter to xAI demanding stronger action to prevent its chatbot, Grok, from generating nonconsensual intimate images and child sexual abuse material distributed on the X platform. The AGs argued that xAI's existing safeguards are insufficient and demanded that the company explain how it will permanently eliminate Grok's ability to create this content, remove existing harmful material, and suspend responsible users. The letter cautioned that Grok's outputs may already violate existing state and federal civil and criminal laws. xAI has not released a public statement regarding the AG coalition's letter and requests.

IV. Surveillance pricing

Surveillance pricing is an emerging practice in which businesses use consumers' personal data to set targeted, individualized prices. Drawing on information such as location, browsing history, and device data, companies may attempt to infer each consumer's willingness to pay and charge accordingly.

California's privacy and consumer protection regulators have launched an investigative sweep into how major retailers, grocers, and hotels use personal data for individualized pricing, specifically warning that undisclosed uses may violate the California Consumer Privacy Act's transparency requirements.

New York has complemented this approach with the Algorithmic Pricing Disclosure Act, which requires businesses using personalized pricing to display a clear notice — "THIS PRICE WAS SET BY AN ALGORITHM USING YOUR PERSONAL DATA" — and authorizes civil penalties for noncompliance.

Together, these initiatives show that state enforcers are pairing investigative powers with affirmative disclosure mandates. Companies using AI-driven pricing should review whether their disclosures are adequate under applicable state privacy and consumer protection laws.

V. Key takeaways for companies

The consistent lesson from recent state AG enforcement activity is that regulators will evaluate AI through traditional legal frameworks — consumer protection, professional licensing, privacy, and advertising law. Companies should be prepared to demonstrate that their governance, disclosures, testing, and oversight are sufficient to prevent consumer harm.

In practical terms, that means substantiating claims about AI performance and accuracy before making them; clearly disclosing uses of personal data, including in pricing; and reviewing AI-generated consumer-facing content for deception. Companies should also implement and document reasonable safeguards against foreseeable misuse, particularly where AI tools may affect children, vulnerable users, or regulated professional advice.

These foundational steps will serve companies well not only under existing state law, but as states continue enacting AI-specific legislation in the months and years ahead.

Ashley Taylor and Clayton Friedman are regular, joint contributing columnists on state attorneys general practice for Westlaw Today and Reuters Legal News.

About the authors

Ashley Taylor (L) is co-leader of **Troutman Pepper Locke**'s state attorneys general practice, vice chair of the firm, and a partner in its regulatory investigations, strategy and enforcement (RISE) practice group He is based in Washington, D.C., and can be reached at ashley.taylor@troutman.com. **Clayton Friedman** (C) is a partner at the firm. His practice involves guiding companies with regulatory challenges, including marketing, advertising, and unfair or deceptive practices. He is based in Orange County and can be reached at clayton.friedman@troutman.com. **Daniel Waltz** (R) is an associate at the firm who focuses his practice on the intersection of industry and government. He regularly counsels clients in connection with government procurement and compliance issues, including Federal Acquisition Regulations (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS), domestic preference, mergers and acquisitions, and small business issues. He is based in Chicago and can be reached at daniel.waltz@troutman.com. Kyara Rivera Rivera, an associate at the firm, contributed to this article.

This article was first published on Reuters Legal News and Westlaw Today on July 27, 2026.