

AI Legal Landscape: Top Challenges and Strategies in 2025 | ArentFox Schiff

Dan Jasnow, Matthew Berlin, Michael Fainberg, Michael Scarpati, Ph.D., D. Reed Freeman Jr., Andrea M. Gumushian, Michelle R. Bowling

While the Trump Administration seems poised to ease regulatory scrutiny on AI, much remains uncertain about their approach. Meanwhile, federal inaction is likely to invite more assertive policymaking at the state and local levels, with a focus on safety, bias, privacy, and sensitive use cases like employment, health care, and education, to name a few. Already, state data transparency laws in California and Colorado are poised to impose new levels of scrutiny on AI developers and deployers before the end of the year, with others such as the European Union's AI Act's first phase of restrictions on prohibited AI systems taking effect just days ago. Understanding the evolving legal landscape and compliance obligations will be critical for GCs to succeed as businesses continue to implement AI.

The Agentic Era

Much has already been written about 2025 ushering in the “agentic era” of AI, but what does this mean for legal compliance? AI agents are typically described as sophisticated AI assistants, capable of acting on the user's behalf. Imagine, for example, asking ChatGPT or Gemini not just to develop a travel itinerary, but also to book your flights, rental car, accommodations, and dinner reservations. Developers and deployers of AI agents should carefully consider risk allocation and liability for the actions of AI agents. For example, if an AI agent inadvertently books the wrong flight, who is liable for the fare? How developers balance the strong desire for powerful automated agents against the safeguard of robust human supervision will be a defining choice for many. Agents could also force a re-imagining of the online business model, with businesses that rely on clicks and views increasingly deprived of the human eyeballs that drive their revenue.

Trust and Safety

[Recent lawsuits against Character.AI](#) showed the consequences of rushing an AI product to market without appropriate safeguards, particularly for tools that engage directly with consumers through conversational interfaces. If not already in place, in-house counsel may want to consider adding a trust and safety program to their 2025 to-do list. While it will differ for each tool, a comprehensive trust and safety program may include a quality assurance program involving human review of model performance and outputs, strong terms of use, a privacy policy that considers users under the age of 13 (if any), an intellectual property (IP) policy that addresses infringing outputs and user generated content, and a policy that outlines how you will deal with sensitive topics like self-harm. Collectively, these policies may help reduce the risk of facing the type of negligence and design defect claims pending against Character.AI.

Federal (In)Action

On January 23, President Trump issued an Executive Order (EO) titled “Removing Barriers to American Leadership in Artificial Intelligence,” which builds on his day-one repeal of the Biden

Administration's EO 14110. The order revokes certain existing AI policies that it claims act as barriers to American AI innovation but does not identify the impacted policies and directives. The order also directs a review of all actions taken pursuant to the now-revoked EO 14110 (Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence). Developers and deployers are unlikely to experience any immediate effects of the revocation of EO14110 or the issuance of Trump's EO on AI. However, both actions suggest that the new Administration will continue to take a hands-off approach to regulating AI and add a layer of uncertainty to the federal regulatory landscape.

Training Data Transparency

No later than January 1, 2026, AI developers will need to start disclosing key information about their training data to comply with California's AI Training Data Transparency Act. Among other things, developers will need to disclose whether their training data contains content owned by third parties and personally identifiable information. Under a similar Colorado law, they will need to provide high level summaries of the type of data used to train their systems. To prepare for these compliance deadlines, developers may consider taking inventory of their training data, comparing it against these statutory disclosure requirements, identifying gaps, and developing processes to ensure that they are adequately tracking changes to or new additions to their data sets, including the impact of retrieval-augmented generation data.

DeepSeek and the Open Source Argument

For several years now, a debate has been raging within the AI developer community over the relative advantages of closed source and open source AI models. With an open source model, information such as source code and the model's weight parameters are made public, allowing any developer to build and innovate upon the work that has come before. With closed source models, such information is typically treated as proprietary or trade secret information. Developers of open source models have argued that open source tools speed innovation, increase efficiency, and reduce development costs, whereas developers of closed source models have argued, among other things, that AI is too powerful to release to the public without robust safeguards and restrictions. With the release of DeepSeek, an open source model that has seemingly matched the capabilities of some of the most powerful AI models at a fraction of the cost, many developers and investors are likely to take a second look at the open source model. The legal implications are also profound, impacting IP valuations, regulatory scrutiny, and product safety.

Winter Is Coming

By the end of 2024, there were nearly 30 active lawsuits alleging that the methods AI developers have used to train AI models violates US copyright law, either because the developers relied on copyrighted content they don't have rights to, and/or removed copyright management information from that content. While these lawsuits took a few steps forward in 2024, no court has issued a definitive ruling on the core legal questions. Whenever that court decision arrives, it could trigger massive statutory damages and a wholesale reimagining of how developers source content for AI training purposes.

The "Sensitive" Use Cases

While the federal regulatory landscape may become more forgiving under the Trump Administration, expect state regulatory action to accelerate in 2025, particularly in blue states

seeking to show leadership on AI safety. If past is prologue, certain use cases — employment, health care, medical device, and education — are likely to face the most scrutiny from lawmakers, regulators, and plaintiffs’ counsel. In addition to AI-specific laws and regulations, AI models or apps in these areas must also comply with industry-specific laws, such as the Family and Medical Leave Act, Health Insurance Portability and Accountability Act, US Food and Drug Administration regulations, and the Family Educational Rights and Privacy Act. Certain use cases may also require annual bias and impact assessments. Developers in these and other high-scrutiny industries should consider conducting compliance audits and developing compliance plans.

To Patent or Not to Patent

AI tools raise challenging questions about how best to protect new inventions. In addition to the fact that software has historically been difficult to patent, software patents may also cause public disclosure of source code and other proprietary information or data. The use of third-party models or open source software further complicates the patentability question. While patent protection may still be the best option for some clients, those proceeding without patent protection should consider whether they have instituted adequate internal safeguards to be able to assert trade secret protection over confidential source code, training data, model weighting parameters, and other sensitive information.

Data Privacy

In the absence of comprehensive federal privacy legislation, an ever-growing number of states have enacted privacy laws that regulate how companies can collect and process personal information. AI companies must be especially careful to consider data flows between app developers and third-party model developers and ensure that privacy policies accurately inform end users of who will have access to their personal information and whether it will be used to train AI models. Privacy policies must also meet increasingly detailed disclosure requirements, including disclosures to end users regarding their rights associated with their personal information. Violations of state privacy laws can have significant consequences with civil and criminal penalties. The Federal Trade Commission (FTC) has also been using its enforcement authority to act against AI developers engaging in alleged “unfair or deceptive acts and practices in or affecting commerce.” To help avoid FTC scrutiny, AI companies should ensure they are not making unsubstantiated claims about their AI tools or that the use of these tools results in bias or discriminatory results.