PUBLICATION

2026 AI Legal Forecast: From Innovation to Compliance

Authors: Edward D. Lanquist, Jr, Alexandra P. Moylan

January 06, 2026

If 2024 was the year of artificial intelligence (AI) hype, 2025 was the year of AI accountability. The legal landscape shifted from theoretical debates to concrete enforcement actions and compliance deadlines. Organizations must now move beyond deploying AI to actively governing it. Regulators in the EU and U.S. are enforcing new standards, and courts are approaching decisions on pivotal copyright cases. This alert identifies the ten legal issues defining the AI landscape that your legal and compliance teams should prioritize.

Intellectual Property and Liability

The Copyright Fair Use Reckoning

Litigation involving major content creators, including *NYT v. OpenAI* and *Getty v. Stability AI*, is entering decisive phases. Courts are beginning to signal whether training on copyrighted data constitutes fair use. Adverse rulings against AI developers could increase pressure for licensing regimes or other significant remedial measures, including potential limits on model deployment. Organizations should audit their use of generative AI tools to distinguish between input risks from data scraping and output risks from generating infringing content.

The Rise of Agentic AI Liability

AI has evolved from chatbots to autonomous agents capable of executing code, signing contracts, and booking transactions. Traditional agency law is being tested. If an AI agent executes a disadvantageous contract, is the user bound by it? Courts are scrutinizing whether users or developers bear liability for autonomous errors. **To date, courts have not issued definitive rulings allocating liability for fully autonomous agent behavior.** Organizations should review vendor contracts for AI agents to ensure indemnification clauses specifically address autonomous actions and hallucinations resulting in financial loss.

Deepfakes and Right of Publicity

Following the 2024 election cycle, legislative momentum has shifted toward protecting individuals from unauthorized synthesized likenesses through measures such as the proposed No FAKES Act. Companies facing imposter fraud from AI voice spoofing in banking and insurance face **heightened litigation and regulatory risk**. Organizations should update identity verification protocols to include multifactor authentication that does not rely solely on voice or video.

Regulatory Compliance

EU AI Act Compliance

The EU AI Act has entered its phased implementation period. As of August 2025, obligations for general-purpose AI (GPAI) models have taken effect. Providers of foundation models must publish detailed summaries of training data, and downstream users must ensure their systems do not fall into prohibited categories such as untargeted facial scraping. Organizations operating in the EU should verify that AI vendors are GPAI-compliant to avoid supply chain disruptions.

The U.S. State Law Patchwork

In the absence of a federal AI bill, states such as California, Utah, Texas, and Colorado have filled the void. The Colorado AI Act is scheduled to become effective in June 2026. Although it remains to be seen what amendments to the legislation will be made, the reasonable care impact assessments required by the law take months to prepare, and those within scope should continue readiness planning. California has enacted health care-adjacent AI legislation, with certain provisions already in effect or coming online in stages. The Texas Responsible Artificial Intelligence Governance Act (TRAIGA), effective January 1, 2026, establishes a comprehensive framework that bans certain harmful AI uses (such as systems designed to incite self-harm, unlawfully discriminate, or produce unlawful deepfakes) and requires disclosures when government agencies and health care providers use AI systems that interact with consumers. The Utah Artificial Intelligence Policy Act requires businesses to clearly disclose when consumers are interacting with generative AI in regulated and certain consumer transactions, and it makes companies liable for deceptive or unlawful practices carried out through AI tools as if they were their own acts. Organizations should not wait for federal preemption and should build compliance programs around the strictest state requirements standards.

Outbound Investment Restrictions

New U.S. Treasury rules regarding outbound investment took effect in early January 2025. U.S. persons are now restricted from investing in foreign entities, specifically in China, developing AI with potential military or surveillance applications. Venture capital and private equity clients must strictly vet portfolio companies for exposure to restricted foreign AI development.

Corporate Strategy and Ethics

Antitrust Scrutiny of AI Acquisitions

Regulators including the Federal Trade Commission (FTC), Department of Justice (DOJ), and the U.K.'s Competition and Markets Authority (CMA) are investigating pseudo-mergers where Big Tech firms hire a startup's leadership and license their intellectual property (IP) to bypass Hart-Scott-Rodino (HSR) merger review. Such deals may be unwound or penalized if found to foreclose competition or monopolize computer resources. Organizations should structure AI partnerships and talent acquisitions carefully to demonstrate they are not attempts to circumvent merger control.

Employment Law and Bias Audits

The U.S. Equal Employment Opportunity Commission (EEOC) and local jurisdictions such as New York City are ramping up enforcement against AI used for hiring and performance tracking. Using resume-screening algorithms without bias audits can lead to class-action exposure under Title VII and the Age Discrimination in Employment Act of 1967 (ADEA). Organizations should require third-party bias audits where required by law or appropriate as a risk-management measure for any automated employment decision tools used in their human resources departments.

Data Privacy and the Right to Unlearn

Privacy regulators are increasingly questioning the permanence of large language models. It is legally disputed whether deleting a user's data from a database is sufficient if that data remains embedded in the model's trained weights. Organizations should update privacy policies to transparently disclose the technical limitations of deletion requests regarding trained AI models.

Professional Responsibility

State bars have begun signaling – and in some cases initiating – disciplinary action related to improper use of AI tools. Using public AI tools for client work without human-in-the-loop verification is now a clear ethical violation. Organizations should implement firm-wide or company-wide AI acceptable use policies that strictly prohibit inputting confidential data into public, non-enterprise AI models.

Recommended Actions for General Counsel and Compliance Officers

Establishing AI governance and compliance programs now will mitigate risk and help your organizations maximize investment in AI solutions. We recommend that you:

1. Inventory AI assets across your organization. You cannot govern what you do not know, so map all shadow AI use across the enterprise.
2. Update vendor agreements to shift liability for IP infringement and autonomous errors back to AI providers.
3. Prepare for compliance with the strictest state regulations and continue to monitor state legislative action.
4. Establish internal incident-response protocols for AI-related errors, hallucinations, or regulatory inquiries.

For further analysis tailored to your sector and compliance footprint, please contact the authors – Edward D. Lanquist or Alexandra (Alex) Moylan, CIPP/US, AIGP – or another member of Baker Donelson's AI Team.