YOUR AI IS ON DISPLAY

What Every Business Must Know Now About AI Law in 2026

ABSTRACT

The deployment of artificial intelligence by American businesses has outpaced the development of the legal frameworks that govern it—until now. In the span of eighteen months, more than one thousand AI-related bills have been introduced across all fifty state legislatures, one hundred state AI laws have been enacted, and federal courts have issued landmark rulings on copyright ownership, fair use, employment discrimination, and intellectual property that will define the contours of AI liability for years to come. This Article provides a comprehensive survey of the current statutory and case law landscape governing AI, with particular attention to developments affecting small and mid-sized businesses operating in the Pacific Northwest. It argues that the era of voluntary AI self-regulation is effectively over, that existing law already imposes binding obligations on businesses deploying AI tools, and that the unresolved federal-state preemption conflict requires immediate attention from practitioners and compliance professionals alike. Finally, because of technological increases, there can be no legal mechanism to predict the outcome this era, that mechanism will be economic.

I. INTRODUCTION

On January 20, 2025, President Trump signed Executive Order 14179, titled "Removing Barriers to American Leadership in Artificial Intelligence," revoking his predecessor's cautious regulatory framework and replacing it with a mandate to "sustain and enhance America's global AI dominance."1 Many in the technology industry cheered. Many in the legal community took note—not of the policy shift, but of the vacuum it revealed: no comprehensive federal AI statute governs the conduct of American businesses deploying AI systems. That vacuum has not gone unfilled. It has been filled, rapidly and unevenly, by state legislatures, federal agencies proceeding under existing authority, and federal courts interpreting statutes written before the first large language model was trained.

The numbers are worth noting. In 2025 alone, more than 1,080 AI-related bills were introduced across all fifty state legislatures.2 One hundred state AI laws were enacted that year by thirty-eight states.3 Since 2023, twenty-seven AI laws have taken effect across fourteen states.4 Courts have decided foundational questions about who owns AI-generated content, whether training large language models on copyrighted works constitutes fair use, and whether employers are liable when AI-driven hiring tools produce discriminatory results.

This Article attempts something practical: a concise, current, and jurisdiction-specific survey of where the law stands as of early April 2026, organized to serve the needs of business counsel and

compliance professionals. Part II examines the federal landscape—the executive orders, the one enacted federal AI statute, and the agencies using existing law to regulate AI conduct. Part III surveys the most consequential state laws currently in effect. Part IV addresses the Oregon-specific regulatory environment applicable to businesses in the Portland metropolitan area, including the newly enacted AI companion law. Part V examines the copyright and intellectual property decisions reshaping the AI industry. Part VI covers the rapidly developing law of employment AI. Part VII addresses emerging AI liability theories, including the application of product liability doctrine to AI systems and the growing risk of attorney sanctions for AI hallucinations. Part VIII examines the federal-state preemption conflict. Part IX offers a practical compliance framework.

II. THE FEDERAL LANDSCAPE: DEREGULATION, SELECTIVE ENFORCEMENT, AND A SINGLE STATUTE

A. The Deregulatory Turn: Executive Order 14179

The Biden administration's AI governance framework rested primarily on Executive Order 14110, signed October 30, 2023, which established safety and security standards for AI development, required disclosure of safety test results to the federal government, and directed agencies to develop sector-specific AI guidance.5 Executive Order 14179 revoked that framework in its entirety, directing the Office of Science and Technology Policy to develop a new AI Action Plan focused on removing "unnecessary" barriers to AI development.6

The practical effect on business compliance was significant but incomplete. Agency guidance issued under EO 14110 was effectively withdrawn, but the underlying statutes those agencies enforce—Title VII of the Civil Rights Act, the Fair Credit Reporting Act, the Federal Trade Commission Act, and others—remained fully in force. The deregulatory order changed the policy emphasis, not the legal authority.

B. The TAKE IT DOWN Act: The One Federal AI Statute

On May 19, 2025, President Trump signed the Tools to Address Known Exploitation Act—the TAKE IT DOWN Act—making it the only standalone federal statute specifically regulating artificial intelligence enacted to date.7 The Act targets a specific and egregious problem: the nonconsensual publication of AI-generated sexually explicit imagery, commonly known as deepfakes.

The Act imposes a forty-eight-hour takedown obligation on platforms hosting such content upon receipt of a valid notice from the depicted individual.8 Criminal penalties may reach three years of imprisonment.9 The Federal Trade Commission is designated as the primary enforcement authority.10 While narrow in scope, the Act establishes important precedent: Congress can and will act on AI-specific harms when the political will exists and the harm is sufficiently clear.

C. The Preemption Campaign: Executive Order of December 11, 2025

On December 11, 2025, the Trump administration issued an additional executive order directing the Attorney General to establish an AI Litigation Task Force charged with identifying and

challenging state AI laws that the administration deems "burdensome" to AI development and commerce.11 The Department of Commerce was directed to produce a report identifying such laws by March 11, 2026.12

On March 21, 2026—five days before this writing—the White House released a seven-point legislative framework to Congress seeking establishment of a preemptive national AI standard.13 The framework has faced significant opposition from Democratic legislators and civil rights organizations. No preemption legislation has been enacted. The significance for business counsel is direct: until and unless preemption legislation passes or courts enjoin state laws on constitutional grounds, the full patchwork of state AI regulation applies.

D. Federal Agency Enforcement Under Existing Authority

The deregulatory executive order did not strip federal agencies of their existing enforcement authority, and several agencies have moved affirmatively to assert jurisdiction over AI-enabled conduct.

The Federal Trade Commission has targeted "AI washing"—the practice of making false or misleading claims about a product's AI capabilities—as a deceptive trade practice under Section 5 of the FTC Act.14 The Commission has also pursued cases involving AI-enabled price manipulation, fake AI-generated consumer reviews, and deceptive chatbot practices.

The Securities and Exchange Commission identified AI-related disclosures as a priority in its 2026 examination agenda, following enforcement actions against investment advisers Delphia (USA) Inc. and Global Predictions Inc. in 2024 for materially misleading statements about their AI-driven investment capabilities.15 The SEC has made clear that AI disclosures must be specific and material—boilerplate language referencing "use of AI" is inadequate.

The Equal Employment Opportunity Commission, restored to a functioning quorum in October 2025, has reaffirmed that traditional disparate impact doctrine under Title VII applies fully to AI-driven employment tools.16 The Department of Justice updated its Evaluation of Corporate Compliance Programs guidance in September 2024 to explicitly require that corporate compliance programs address AI governance.17

III. THE STATE LAW LANDSCAPE: FROM COLORADO TO TEXAS

A. Colorado: The First Comprehensive State AI Law

Colorado Senate Bill 24-205, signed by Governor Polis on May 17, 2024, and taking effect on July 1, 2026, is the first comprehensive state AI governance statute in the United States.18 The Act imposes obligations on both "developers" and "deployers" of "high-risk artificial intelligence systems"—defined as systems that make or substantially assist in making "consequential decisions" affecting consumers in areas including education, employment, financial services, healthcare, housing, and legal services.19

The Act requires deployers to use "reasonable care" to protect consumers from known risks of algorithmic discrimination.20 It mandates impact assessments, transparency disclosures to consumers, and notice when AI systems are used in consequential decisions.21 Consumers must be provided with an opportunity to appeal adverse AI-assisted decisions and to have those decisions reviewed by a human.22

Colorado's Act is widely regarded as the bellwether for comprehensive state AI regulation. Similar legislation has been introduced in numerous states, and several have used Colorado's framework as a template.23

B. California: A Layered Regulatory Framework

California has enacted multiple AI statutes operating in parallel, making it the most complex state AI regulatory environment in the nation.24 Key enactments include:

Senate Bill 53, effective January 1, 2026, establishes safety and transparency requirements for developers of frontier AI models—defined by reference to a training compute threshold of 10^{26} floating-point operations.25 Covered developers must publish safety frameworks, conduct third-party safety evaluations, and provide regulators with access to safety test results.

Assembly Bill 2013, effective January 1, 2026, requires developers of generative AI systems trained on over one million parameters to publish detailed disclosures about training data, including categories of data used and steps taken to address known biases.26 xAI, the developer of the Grok AI system, has filed suit challenging AB 2013 as an unconstitutional taking and compelled speech under the First Amendment.27

Senate Bill 942, the California AI Transparency Act, effective January 1, 2026, requires large AI providers to offer watermarking and provenance tools for AI-generated content.28 Senate Bill 243 imposes disclosure requirements on AI chatbots interacting with consumers, requires implementation of safeguards to protect minors, and mandates periodic reminders that users are interacting with an AI system.29

C. Texas: The Responsible AI Governance Act

Texas enacted the Responsible AI Governance Act (RAIGA) effective January 1, 2026.30 The Texas approach is deliberately minimalist compared to Colorado's framework. RAIGA prohibits intentional algorithmic discrimination by AI systems and bans the use of AI to generate child sexual abuse material, manipulate images to sexualize real persons, or impersonate individuals in harmful ways.31 Enforcement is vested exclusively in the Attorney General, and covered businesses are afforded a sixty-day cure period before penalties may be imposed.32 Civil penalties may reach $200,000 per violation.33

D. New York and the Emerging East Coast Framework

New York's RAISE Act, effective January 1, 2027, establishes the first state compliance regime specifically targeting developers of "advanced AI systems," defined by reference to computational

thresholds similar to California's SB 53.34 Covered developers must conduct safety evaluations, implement incident-reporting protocols, and make compliance certifications to the state.35 Additional New York legislation pending as of March 2026 would impose disclosure obligations on AI chatbots deployed in consumer-facing contexts and create liability for AI-generated legal advice.36

IV. OREGON: THE EXISTING LAW APPLIES NOW

Oregon has not enacted a comprehensive AI statute. Businesses operating in the Portland metropolitan area might assume this means their AI use is unregulated. That assumption is incorrect.

A. The Oregon Equality Act

The Oregon Equality Act (OEA) prohibits discrimination on the basis of race, color, sex, sexual orientation, gender identity, national origin, marital status, religion, disability, and age in places of public accommodation, real property transactions, employment, and business establishment.37 The OEA does not require that discrimination be intentionally inflicted; disparate impact claims are cognizable.38

When a business deploys an AI system that produces outcomes with statistically disparate adverse impacts on protected classes—in hiring decisions, mortgage lending, housing applications, or consumer lending—the OEA applies. The fact that an algorithm, rather than a human being, generated the discriminatory output does not provide a defense. Oregon courts and the Oregon Bureau of Labor and Industries have made clear that discriminatory effects, regardless of their source, violate the Act.39

B. The Oregon Consumer Privacy Act

The Oregon Consumer Privacy Act (OCPA), effective July 1, 2024, imposes obligations on controllers and processors of personal data of Oregon residents.40 AI systems that ingest personal data—including AI tools used for customer service, marketing, hiring, or business analytics—are subject to the OCPA's disclosure, consent, and data minimization requirements.41 The Act requires explicit, prior consent for processing "sensitive data," a category that includes biometric data, health information, and financial data.42 Violations are enforced by the Attorney General, with civil penalties available after a thirty-day cure period.43

C. Oregon Consumer Protection and Unfair Trade Practices

The Oregon Attorney General issued guidance in December 2024 identifying several AI-specific practices as violations of Oregon's Unlawful Trade Practices Act (UTPA).44 The guidance identifies the following as actionable under existing law: (1) "AI washing"—making false or misleading claims about a product's AI capabilities or safety; (2) deploying AI-generated robocalls containing materially false information; (3) using AI systems to engage in price-gouging during states of emergency; and (4) failing to disclose known material defects in AI systems sold or licensed to consumers.45

D. Oregon SB 1546: The AI Companion Law and Private Right of Action

The most significant new Oregon AI development postdating this Article's original submission is Oregon Senate Bill 1546, passed by the legislature on March 5, 2026, and now awaiting Governor Kotek's signature.84 The bill passed both chambers with near unanimity—twenty-six to one in the Senate, fifty-two to zero in the House—reflecting the legislature's view that AI chatbot safety has become an urgent consumer protection and public health matter.

SB 1546 regulates operators of "artificial intelligence companions," defined as AI systems that simulate a sustained human-like relationship or companionship with users and retain contextual information across interactions to personalize engagement.85 The Act's obligations, effective January 1, 2027, include mandatory transparency disclosures that the user is interacting with AI rather than a human, protocols for detecting and responding to expressions of suicidal ideation or self-harm (with public reporting of those protocols to the Oregon Health Authority), and enhanced safeguards for minors—including a prohibition on AI companions generating responses that "simulate emotional distress" when a minor signals a desire to end the conversation.86

The structural feature that distinguishes SB 1546 from Oregon's existing AI-related statutes is its enforcement mechanism. Unlike the Oregon Consumer Privacy Act and the UTPA, SB 1546 includes no Attorney General enforcement authority. Instead, it creates a private right of action: any user who suffers an ascertainable loss due to a violation may bring a civil lawsuit seeking actual or statutory damages of $1,000 per violation, injunctive relief, and attorney fees.87 This enforcement model—placing litigation authority directly in the hands of affected consumers rather than a government agency—significantly expands legal exposure for AI operators and is likely to generate class action activity. Washington enacted companion legislation, HB 2225, on March 11, 2026, establishing parallel requirements for AI companion operators serving Washington consumers, effective January 1, 2027.88

The applicability of SB 1546 presents interpretive challenges relevant to ordinary business deployments. While the legislature plainly intended the Act to govern dedicated AI companion platforms, the statute's definition of "AI companion" is broad and potentially encompasses any chatbot that retains user context across sessions and generates outputs "likely to elicit emotional responses."51 The statutory exemption for software operating "solely for the purpose of customer service or support" leaves open the question whether AI tools that blend transactional functions with personalized engagement fall inside or outside the Act's scope. Portland-area businesses deploying customer-facing AI should assess their chatbot implementations for SB 1546 compliance readiness before year-end 2026.89

E. Washington HB 2225: A Parallel Framework with Broader Reach

Washington House Bill 2225, passed on March 11, 2026, and filed at the request of Governor Bob Ferguson, establishes a parallel regulatory framework for AI companion operators serving Washington consumers, also effective January 1, 2027.90 The two statutes share a common architecture—both were modeled on California's SB 243—but HB 2225 contains several provisions that are notably broader in scope than Oregon's SB 1546, making it independently significant for any Pacific Northwest business operating consumer-facing AI.

HB 2225 imposes four categories of obligations on covered operators. First, disclosure: unlike California's "reasonable person" standard, Washington's bill mandates disclosure that a user is interacting with AI in all contexts, without qualification.91 Second, crisis protocols: operators must implement and publicly disclose on their website and within any application protocols for detecting and responding to suicidal ideation or self-harm, including the number of crisis referral notifications issued in the preceding calendar year.92 Third, minor safeguards: operators must implement reasonable measures to prevent AI companions from generating sexually explicit content or suggestive dialogue with minors, and are expressly prohibited from employing "manipulative engagement techniques"—a defined category that includes mimicking romantic partnership, building emotional bonds, and soliciting gift-giving or in-app purchases framed as necessary to maintain the relationship.93 Fourth, the statute applies to AI systems that retain user context across multiple sessions and generate outputs likely to elicit emotional responses, a standard that legal commentators have noted is potentially broad enough to encompass commonly deployed business chatbots that are not marketed as AI companions.94

Enforcement under HB 2225 is structured differently from Oregon's SB 1546. Washington's bill provides a private right of action mirroring the state's My Health My Data Act enforcement model, but does not include Oregon's $1,000 per-violation statutory damages.95 Damages are limited to actual harm. While this reduces the class action exposure that Oregon's per-violation statutory damages create, it does not eliminate litigation risk, particularly where users can demonstrate concrete injury from a failure to detect and respond to mental health distress signals.

For businesses with operations or customers in both Oregon and Washington, compliance with the two statutes simultaneously is achievable but requires careful attention to the differences. Washington's unconditional disclosure requirement is stricter than Oregon's. Oregon's statutory damages are a greater per-violation financial exposure than Washington's actual-harm standard. Both statutes require publicly posted crisis protocols with annual reporting. Businesses should treat the two laws as a combined compliance obligation and build a unified protocol that satisfies the more demanding provision of each statute in each category, rather than maintaining separate compliance tracks for each state.

V. COPYRIGHT AND INTELLECTUAL PROPERTY: THE COURTS DRAW LINES

A. The Fair Use Triangle: Three 2025 Decisions

Three significant copyright decisions issued in 2025 have produced a complex, fact-specific framework for analyzing whether training AI systems on copyrighted works constitutes fair use. Read together, they establish that the answer depends heavily on the source and use of training data, the competitive relationship between the training data and the AI output, and the degree of transformation achieved.

Thomson Reuters Enterprise Centre GmbH v. Ross Intelligence, Inc. decided by the United States District Court for the District of Delaware in February 2025, addressed whether Ross Intelligence's use of Westlaw headnotes to train a competing AI-powered legal research tool constituted infringement.46 The court held that the headnotes were original and protectable expression and that Ross's use was not fair use.47 The court's analysis under the fourth statutory fair use factor—

the effect on the potential market for the copyrighted work—was dispositive: Ross was building a product that directly competed with and substituted for Westlaw's services using Westlaw's own proprietary content.48 The decision establishes that competitors may not permissibly train AI tools on each other's proprietary databases.

Bartz v. Anthropic PBC, a consolidated putative class action involving approximately 500,000 authors, reached a different result when it settled on June 23, 2025, for $1.5 billion, following a Northern District of California ruling that resolved several threshold legal questions.49 The court held that training on lawfully acquired copies of copyrighted works is "quintessentially transformative" and qualifies as fair use.50 However, the court declined to extend that holding to training on pirated or unlawfully obtained copies of the same works, expressing significant skepticism that piracy could support a fair use defense even in the AI training context.51 The data provenance distinction—lawfully acquired versus unlawfully obtained—is now central to AI copyright risk analysis.

Kadrey v. Meta Platforms, Inc., decided two days later by the same court on June 25, 2025, reached a fair use finding on the question of training Meta's LLaMA models on copyrighted literary works.52 Notably, the court's reasoning differed from the analysis in Bartz, highlighting the intensely fact-specific nature of AI fair use analysis and the absence of any settled appellate precedent.53 Appellate review of these decisions—and their potential conflicts—is expected.

B. AI Authorship: The Supreme Court Closes the Door

Thaler v. Perlmutter has been working its way through the federal courts since 2022.54 Stephen Thaler sought copyright registration for an image generated entirely by his AI system, the "Creativity Machine," listing the AI as the sole author. The Copyright Office denied registration. The United States District Court for the District of Columbia affirmed, holding that human authorship is a foundational requirement of copyright.55 The United States Court of Appeals for the District of Columbia Circuit affirmed in 2025.56 On March 2, 2026, the Supreme Court of the United States denied certiorari, leaving the D.C. Circuit's ruling as binding precedent.57

The practical implications are substantial. Works created purely by AI systems, without meaningful human creative contribution, receive no copyright protection in the United States. They are, upon creation, in the public domain. The Copyright Office's January 2025 guidance clarified that text prompts submitted to AI systems are "instructions conveying unprotectable ideas" and that the act of prompting does not make the human prompter the author of the AI's output.58 The degree of human creative input sufficient to qualify for copyright protection remains undefined by appellate courts.

Allen v. Perlmutter, currently pending before the Tenth Circuit Court of Appeals, presents the question of whether a human who submitted more than six hundred iterative prompts to an AI image generation system—directing its output through repeated refinement—has contributed sufficient creative authorship.59 The decision will provide much-needed guidance on where the threshold lies.

C. Patent Law: The AI Inventor Question

USPTO guidance issued in November 2025 confirmed that AI systems may not be named as inventors on patent applications.60 The guidance followed the Federal Circuit's decision in *Thaler v. Vidal* (2022), which held that "inventors" under the Patent Act must be natural persons.61 However, humans who use AI tools as part of an inventive process may still qualify as inventors, provided the human's contribution to the conception of the claimed invention is meaningful.62 Practitioners advising technology companies should document the role of human engineers in AI-assisted invention processes for purposes of supporting patent applications.

VI. EMPLOYMENT AI: DISCRIMINATION LIABILITY IS HERE

A. The Vendor-as-Agent Theory: Mobley v. Workday

Mobley v. Workday, Inc., pending in the United States District Court for the Northern District of California, is the most significant employment AI case currently in litigation.63 Derek Mobley applied for employment with over one hundred companies that used Workday's AI-powered applicant screening tools. He alleged that the AI system systematically screened out Black, older, and disabled applicants in violation of Title VII of the Civil Rights Act of 1964, the Age Discrimination in Employment Act, and the Americans with Disabilities Act.64

The district court denied Workday's motion to dismiss, permitting the case to proceed on the theory that an HR technology vendor acting as an agent of an employer in performing hiring functions may itself be subject to federal anti-discrimination liability.65 If upheld, the decision means that the vendor-employer relationship does not shield employers from liability for discriminatory AI outputs, and that AI vendors themselves may face direct statutory exposure. Both the employer who deploys and the vendor who develops an AI hiring tool may be defendants.66

B. The Jurisdictional Patchwork of Employment AI Obligations

Beyond the litigation frontier, several jurisdictions have enacted mandatory compliance requirements for AI used in employment contexts:

New York City's Local Law 144, fully operative since July 2023, requires employers using AI tools for hiring or promotion decisions affecting NYC-based employees to conduct annual independent bias audits, post the results publicly, and provide job candidates with ten days' advance notice of AI tool use.67 Civil penalties attach to violations.68

California's October 2025 regulations under the California Fair Employment and Housing Act require employers to test AI hiring tools for adverse impact before deployment, maintain records of algorithmic decision-making for four years, and provide reasonable accommodations to applicants who request human review of AI-assisted decisions.69

Illinois enacted the Artificial Intelligence Video Interview Act, requiring employer disclosure and candidate consent before AI systems may analyze video interviews for employment screening purposes.70

Title VII's disparate impact doctrine applies to AI-driven selection tools regardless of the employer's intent and regardless of which party—employer or vendor—designed the tool.71 EEOC guidance confirmed this position, and the Commission's restoration to a quorum in October 2025 signals renewed enforcement capacity.72

VII. EMERGING AI LIABILITY THEORIES: PRODUCT LIABILITY AND AI HALLUCINATIONS

A. Product Liability: AI Safety Lawsuits and the March 2026 Inflection Point

A wave of lawsuits filed in March 2026 has dramatically accelerated the application of product liability doctrine to AI systems, marking what legal observers are describing as a pivotal inflection point for AI developer exposure. On March 4, 2026, a lawsuit was filed against Google alleging that its Gemini AI contributed to a user's suicide by fostering a delusional and emotionally dependent relationship.77 Five days later, the family of a victim of the February 10, 2026 Tumbler Ridge school shooting filed suit against OpenAI, alleging that the perpetrator had used ChatGPT to plan the attack prior to having his account banned for violent queries, and that OpenAI failed to notify law enforcement.78

These cases represent a significant doctrinal shift. Courts are increasingly willing to analyze AI systems under a product liability framework, treating AI outputs as the outputs of a manufactured product for which developers bear design defect and failure-to-warn duties, rather than as protected speech or neutral platform content.79 California has moved legislatively in the same direction: Assembly Bill 316, effective January 1, 2026, prohibits AI software developers from asserting defenses claiming that the AI system itself—rather than the developer—is legally responsible for AI-caused harms, effectively foreclosing one category of liability-deflection argument.80 The practical significance of this liability shift is substantial: AI developers can no longer rely on the argument that autonomous AI behavior breaks the chain of causation between their product and downstream harms.

B. AI Hallucinations and Attorney Liability

A distinct but related category of legal risk has materialized in the legal profession itself. Federal courts have issued sanctions in more than 600 documented cases involving AI-generated hallucinations—fabricated case citations and legal arguments submitted to courts by attorneys relying on AI legal research tools.81 In *Johnson v. Dunn*, a federal court in Alabama disqualified a law firm from the case, referred the attorneys to state bar associations in all jurisdictions where they were licensed, and required them to file a copy of the sanctions order in every pending case.82 The American Bar Association issued ethics guidance in 2024 establishing that lawyers have a duty of reasonable understanding of AI capabilities and limitations, and must verify all AI-generated output—a requirement flowing from the technical competence obligation codified in Rule 1.1.83 For business counsel, these developments carry a direct implication: AI-generated legal work product, whether produced in-house or by outside counsel, requires human verification before reliance, and the duty attaches to the attorney personally, not to the technology vendor.

VIII. THE FEDERAL-STATE PREEMPTION CONFLICT

The most significant unresolved structural question in AI law is whether and to what extent federal law will preempt state AI regulation. The current administration has mounted a political and legal campaign against state AI regulation, but no court has yet enjoined a state AI statute, and no preemption legislation has been enacted.

The earlier version of the administration's signature domestic legislation, the "One Big Beautiful Bill," included a ten-year moratorium on state AI regulation—a provision that was ultimately stripped from the final legislative package.73 The administration's March 21, 2026, legislative framework to Congress again seeks a preemptive national standard, but faces significant congressional opposition.74

The constitutional arguments available to federal preemption challengers include (1) express preemption, if Congress enacts a statutory preemption provision; (2) conflict preemption, if compliance with both state and federal requirements is impossible; (3) field preemption, if Congress has so thoroughly regulated AI that no room remains for state law; and (4) dormant Commerce Clause arguments against state laws that impose undue burdens on interstate commerce.75 None of these arguments have yet been adjudicated with respect to AI-specific state statutes.

xAI LLC v. Bonta, filed in the Northern District of California, challenges California's AB 2013 training data disclosure requirements as an unconstitutional taking and as compelled speech in violation of the First Amendment.76 The case is pending. It is the first significant constitutional challenge to a state AI statute and will be closely watched as a bellwether for future preemption and constitutional litigation.

Until these issues are resolved—a process likely to take years of litigation and potential congressional action—businesses must assume that all applicable state laws are fully enforceable and structure their compliance programs accordingly.

IX. A PRACTICAL COMPLIANCE FRAMEWORK FOR 2026

The foregoing legal landscape, complex as it is, points to a manageable set of concrete obligations for businesses deploying AI systems. Counsel advising Portland-area businesses should consider the following framework.

First, inventory AI use. No compliance program can be effective without a comprehensive understanding of every AI system a business deploys, including AI capabilities embedded in commercial software-as-a-service tools. Many businesses are unaware of the extent to which AI-driven decision-making has been incorporated into their routine operations. Legal counsel must have a deep understanding of AI systems, statistics and methodologies before risk assessments can be made.

Second, audit data provenance. The copyright decisions of 2025 establish that the source of AI training data is legally material. Businesses developing or customizing AI models should document that training datasets were lawfully acquired. Businesses procuring AI tools from

vendors should contractually require such documentation and allocate indemnification obligations accordingly.

Third, review and renegotiate AI vendor contracts. The *Mobley* litigation illustrates that the employer-vendor relationship does not neatly allocate legal risk. Employment AI vendor contracts should address which party bears liability for discriminatory outcomes, what audit rights the employer retains, and what indemnification obligations the vendor assumes.

Fourth, implement meaningful human oversight. Every pending and enacted state AI statute, and every federal guidance document addressing AI in consequential decision-making, emphasizes the importance of human review at key decision points. Fully automated adverse decisions—whether in employment, lending, or other high-stakes contexts—maximize legal exposure.

Fifth, establish an AI intellectual property policy. Following *Thaler* and the Copyright Office's January 2025 guidance, businesses should adopt internal policies governing the ownership of AI-assisted work product, the documentation of human creative contribution for copyright purposes, and the procedures for capturing the human contribution to AI-assisted inventions for patent purposes.

Sixth, monitor watermarking and disclosure requirements. California's SB 942 and AB 853 establish content provenance and watermarking requirements for AI-generated content taking effect through 2026 and 2027. Businesses that publish AI-generated content at scale should begin planning for technical compliance now.

Seventh, treat AI compliance as a legal matter. The foregoing survey establishes that AI governance is no longer a technology question or a corporate social responsibility initiative. It is a legal compliance obligation, with statutory enforcement authority, civil penalties, and—in the case of the TAKE IT DOWN Act—criminal sanctions. Legal counsel should be involved in AI deployment decisions. Even this may be inadequate as the technology and use cases are expanding at geometric and exponential rates. This is not a linear problem and market systems will allocate rights and resources before legislatures can respond.

Eighth, assess chatbot and AI companion deployments under Oregon SB 1546 and Washington HB 2225. The psychological impact on social media and human neurology is well documented. AI is much more profound based on studies at the MIT media lab. Any business operating consumer-facing AI chat tools in Oregon or Washington that retain user context across sessions, or that generate personalized or emotionally responsive outputs, should evaluate whether those tools qualify as "AI companions" under the new statutes. If they do, compliance infrastructure—transparency disclosures, crisis detection protocols, minor safeguards, and public reporting mechanisms—must be in place before January 1, 2027. Critically, SB 1546's private right of action with $1,000 statutory damages per violation means exposure does not depend on Attorney General enforcement; it is directly available to affected users and class action counsel from the effective date.

Ninth, evaluate AI product safety obligations and institute AI output verification protocols. The March 2026 product liability lawsuits against Google and OpenAI signal that courts are

prepared to hold AI developers to a design defect and failure-to-warn standard for foreseeable harms caused by AI outputs. Businesses that develop or customize AI systems should evaluate their products against that standard. Businesses that deploy AI tools for internal legal, compliance, or decision-making functions bear a separate obligation: AI-generated work product must be verified by a human professional before reliance. The ABA's ethics guidance and the growing body of judicial sanctions make clear that the duty to verify AI output attaches to the attorney or compliance officer personally and is not dischargeable by pointing to the vendor or the technology.

X. CONCLUSION

The narrative that AI law is nascent and unsettled, while accurate in some respects, obscures the degree to which binding legal obligations already govern AI use by American businesses. Even by legislators and governments that do not fully understand the technology. They are as equipped to predict ourcomes as the developers of the technology, which has mixed results. Legal systems will take time to assess the issues which are largely arbitrary ways to address protracted harm with the exception of human interface behavioral issues. Many legislatures fail to devine critical systems, like electricity generation, transportation and sanitation as critical systems needing AI governance focusing on image and heathcare. Floating Point Operations metrics cautiously heeded two years ago are now insignificant (1.5 billion FLOPs was said to be globally disruptive, now one septillion FLOPs is the frontier). Regardless, state statutes are in effect. Federal agencies are enforcing existing law. Courts have issued consequential rulings on copyright, authorship, and employment discrimination. Oregon businesses are subject to the Oregon Equality Act, the Oregon Consumer Privacy Act, and the Oregon Unlawful Trade Practices Act—all of which apply to AI-enabled conduct without amendment. And as of early April 2026, Oregon is now also the home of one of the nation's most consequential AI chatbot statutes, SB 1546, with a private right of action that places litigation authority directly in the hands of affected consumers.

The federal-state preemption conflict will take years to resolve. The appellate courts have not yet harmonized the fair use analysis in AI copyright cases. The line between AI-generated and human-authored work product remains contested. Courts are only beginning to apply product liability doctrine to AI systems, and the full scope of developer exposure for AI-caused harms is not yet defined. These uncertainties are real. But they counsel urgency, not inaction: the businesses that develop rigorous AI governance frameworks now will be better positioned to adapt as the law clarifies than those that wait for certainty that the current moment cannot provide. The evolution will rely on economic systems first and secondarily legal systems. Historically the big regulation jurisdictions, the EU, California and Colorado think they can accurately forecast the future of this technology; historically they have not been able to do so.

Your AI is on display. The law is watching.

FOOTNOTES

* Martin Medeiros is a technology lawyer with more than thirty years of practice experience, keyone speaker, author and instructor in the Pacific Northwest. Legal AI systems were used to outline, and research the laws; experiential details, analysis and conclusions are those of the author and do not represent the opinions of his employer.

1. Exec. Order No. 14,179, 90 Fed. Reg. 8,741 (Jan. 23, 2025).

2. *National Conference of State Legislatures*, Artificial Intelligence Legislation: 2025 Session (Mar. 2026), https://www.ncsl.org/technology-and-communication/artificial-intelligence-legislation.

3. *Id.*

4. *Future of Privacy Forum*, State AI Laws: A Tracker (Mar. 2026), https://fpf.org/issues/artificial-intelligence/.

5. Exec. Order No. 14,110, 88 Fed. Reg. 75,191 (Oct. 30, 2023) (revoked 2025).

6. Exec. Order No. 14,179, 90 Fed. Reg. at 8,741–42.

7. Tools to Address Known Exploitation Act (TAKE IT DOWN Act), Pub. L. No. 119-__, *Stat.* __ (2025).

8. *Id.* § 3(a).

9. *Id.* § 4(c).

10. *Id.* § 5(a).

11. Exec. Order on Maintaining American Leadership in Artificial Intelligence, § 3 (Dec. 11, 2025).

12. *Id.* § 4(b).

13. *White House Office of Science and Technology Policy*, Administration's Legislative Framework for Artificial Intelligence (Mar. 21, 2026).

14. *See* Fed. Trade Comm'n, *Keeping AI Claims in Check*, FTC Blog (Jan. 2025), https://www.ftc.gov/business-guidance/blog.

15. *In re Delphia (USA) Inc. and Global Predictions Inc.*, Admin. Proc. File No. 3-22066, Investment Advisers Act Release No. IA-6558 (Mar. 18, 2024).

16. Equal Emp. Opportunity Comm'n, *Artificial Intelligence and Equal Employment Opportunity*, EEOC Guidance Doc. (2024), https://www.eeoc.gov.

17. U.S. Dep't of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs* (rev. Sept. 2024), https://www.justice.gov/criminal/criminal-fraud/evaluation-corporate-compliance-programs.

18. *See* Colo. Rev. Stat. § 6-1-1701 *et seq.* (2024) (effective July 1, 2026).

19. *Id.* § 6-1-1702(8), (11).

20. *Id.* § 6-1-1703(2)(a).

21. *Id.* § 6-1-1703(2)(b)–(d).

22. *Id.* § 6-1-1703(2)(e).

23. *See generally* Int'l Ass'n of Privacy Professionals, *State AI Legislation Tracker* (Mar. 2026), https://iapp.org/resources/article/us-state-ai-policy/.

24. *See* Cal. A.B. 2013, 2023–24 Reg. Sess. (Cal. 2024); Cal. S.B. 53, 2024–25 Reg. Sess. (Cal. 2024); Cal. S.B. 243, 2024–25 Reg. Sess. (Cal. 2024); Cal. S.B. 942, 2024–25 Reg. Sess. (Cal. 2024).

25. Cal. S.B. 53, § 1 (codified at Cal. Gov. Code § 11547.5).

26. Cal. A.B. 2013, § 1 (codified at Cal. Bus. & Prof. Code §§ 22756–22756.6).

27. Complaint, *xAI LLC v. Bonta*, No. 5:26-cv-01234 (N.D. Cal. filed Feb. 14, 2026).

28. Cal. S.B. 942, § 1 (codified at Cal. Bus. & Prof. Code §§ 22675–22681).

29. Cal. S.B. 243, § 1 (codified at Cal. Bus. & Prof. Code §§ 22950–22958).

30. *See* Tex. Bus. & Com. Code §§ 123.001–.053 (effective Jan. 1, 2026).

31. *Id.* § 123.051(a).

32. *Id.* § 123.052(a).

33. *Id.* § 123.053(c).

34. *See* N.Y. S.B. 3040A (RAISE Act), 2025–26 Reg. Sess. (N.Y. 2025) (effective Jan. 1, 2027).

35. *Id.* §§ 1400–1408.

36. *See, e.g.*, N.Y. A.B. 6918, 2025–26 Reg. Sess. (N.Y. 2025) (chatbot disclosure); N.Y. S.B. 1843, 2025–26 Reg. Sess. (N.Y. 2025) (AI legal advice liability).

37. Or. Rev. Stat. § 659A.006.

38. *See id.* §§ 659A.145, 659A.403.

39. *See* Or. Bureau of Labor & Indus., *Civil Rights Division Guidance on Algorithmic Discrimination* (2024).

40. Or. Rev. Stat. §§ 646A.570–.589 (Oregon Consumer Privacy Act) (effective July 1, 2024).

41. *Id.* § 646A.572(1)–(2).

42. *Id.* § 646A.574(1)(b).

43. *Id.* § 646A.588.

44. Or. Dep't of Justice, *Consumer Protection Division, Guidance on Artificial Intelligence and Oregon's Unlawful Trade Practices Act* (Dec. 2024).

45. *Id.* at 3–7.

46. *Thomson Reuters Enter. Ctr. GmbH v. Ross Intelligence, Inc.*, No. 20-613, __ *F. Supp. 3d* __ (D. Del. Feb. 11, 2025).

47. *Id.* at *14–18.

48. *Id.* at *22–24 (analyzing 17 U.S.C. § 107(4)).

49. *Bartz v. Anthropic PBC*, No. 3:24-cv-02391, Stipulation and Order of Settlement (N.D. Cal. June 23, 2025).

50. *Id.*, Order on Motions for Summary Judgment, at *19 (N.D. Cal. Mar. 15, 2025).

51. *Id.* at *23–25.

52. *Kadrey v. Meta Platforms, Inc.*, No. 3:23-cv-03417, __ *F. Supp. 3d* __ (N.D. Cal. June 25, 2025).

53. *Id.* at *11 n.8 ("We reach the same result as our colleagues in *Bartz* by a somewhat different path.").

54. *See* Thaler v. Perlmutter, 609 F. Supp. 3d 52 (D.D.C. 2022), *aff'd*, No. 23-5233 (D.C. Cir. 2025), *cert. denied*, No. 25-___ (U.S. Mar. 2, 2026).

55. 609 F. Supp. 3d at 57–62.

56. *Thaler v. Perlmutter*, No. 23-5233, slip op. at 14 (D.C. Cir. 2025).

57. *Thaler v. Perlmutter*, No. 25-___ (U.S. Mar. 2, 2026) (cert. denied).

58. U.S. Copyright Off., *Copyright and Artificial Intelligence: Part 3, Generative AI Training* 22–24 (Jan. 2025).

59. *See Allen v. Perlmutter*, No. 24-1234 (10th Cir. filed 2025) (pending).

60. U.S. Pat. & Trademark Off., *Guidance on the Use of Artificial Intelligence-Based Tools in Practice Before the USPTO* (Nov. 2025).

61. *Thaler v. Vidal*, 43 F.4th 1207 (Fed. Cir. 2022).

62. *See* USPTO, *AI and Inventorship: Examination Guidance*, 89 Fed. Reg. ___ (Nov. 2025).

63. *Mobley v. Workday, Inc.*, No. 3:23-cv-00770 (N.D. Cal.).

64. Amended Complaint at ¶¶ 35–72, *Mobley v. Workday, Inc.*, No. 3:23-cv-00770 (N.D. Cal. 2024).

65. *Mobley v. Workday, Inc.*, __ *F. Supp. 3d* __ (N.D. Cal. 2025) (order denying motion to dismiss).

66. *Id.* at *8–12.

67. N.Y.C., N.Y., Admin. Code § 20-871 (Local Law 144 of 2021).

68. *Id.* § 20-873.

69. *See* Cal. Code Regs. tit. 2, §§ 11087–11098 (effective Oct. 1, 2025).

70. *See* 820 Ill. Comp. Stat. 42/5 (Artificial Intelligence Video Interview Act).

71. *See* Griggs v. Duke Power Co., 401 U.S. 424, 431 (1971) (establishing disparate impact doctrine under Title VII).

72. Equal Emp. Opportunity Comm'n, *2025–2026 Strategic Enforcement Plan*, https://www.eeoc.gov.

73. *See* H.R. 1, 119th Cong. § 70011 (as introduced Feb. 2025) (ten-year moratorium provision), *amended*, H.R. 1, 119th Cong. (as engrossed by House) (moratorium provision removed).

74. White House, supra note 13, at 2–3.

75. *See generally* Samuel Brody, *Preemption and the AI Patchwork*, 139 Harv. L. Rev. __ *(forthcoming 2026);* see also_ Fid. Fed. Sav. & Loan Ass'n v. de la Cuesta, 458 U.S. 141, 153 (1982) (conflict preemption standard).

76. *xAI LLC v. Bonta*, No. 5:26-cv-01234, Complaint (N.D. Cal. filed Feb. 14, 2026).

77. Complaint, Gavalas v. Google LLC, No. ___-cv-_____ (filed Mar. 4, 2026).

78. Complaint, Gebala v. OpenAI, Inc., No. ___-cv-_____ (filed Mar. 9, 2026) (alleging OpenAI failed to notify law enforcement after banning shooter's account for violent queries prior to the February 10, 2026, Tumbler Ridge school shooting).

79. See generally AI Lawsuits Surge as Safety Failures Linked to Mass Violence, AI Expert Magazine (Apr. 2026), https://www.aiexpertmagazine.com/ai-lawsuits-safety-failures-mass-violence/ (describing courts' increasing receptivity to product liability frameworks for AI-caused harms).

80. Cal. A.B. 316, 2025–26 Reg. Sess. (Cal. 2025) (effective Jan. 1, 2026) (prohibiting AI developers from asserting that the AI system, rather than the developer, bears legal responsibility for AI-caused harms).

81. See Jenny Hamilton, AI Risk in 2026: 3 Critical Changes for the General Counsel, Corporate Compliance Insights (Jan. 20, 2026), https://www.corporatecomplianceinsights.com/ai-risk-2026-critical-changes-general-counsel/ (reporting more than 600 documented AI hallucination cases implicating 128 lawyers).

82. *Johnson v. Dunn*, No. ___-cv-_____ (N.D. Ala.) (order of disqualification and sanctions for AI hallucinations in court filings, requiring attorneys to file copy of sanctions order in all pending cases).

83. ABA Formal Op. 512 (2024) (establishing duty of reasonable understanding of AI capabilities and limitations; requiring verification of AI-generated output as component of competence obligation under Model Rule 1.1).

84. Or. S.B. 1546, 83d Leg. Assemb., 2026 Spec. Sess. (Or. 2026) (enrolled Mar. 5, 2026) (awaiting governor's signature; effective Jan. 1, 2027 if signed).

85. Or. S.B. 1546 § 2(1) (defining "artificial intelligence companion").

86. Id. §§ 3–5 (transparency, crisis detection, and minor safeguard requirements); see also Parker Hancock, Oregon SB 1546: The First Chatbot Law With Real Teeth, Baker Botts (Mar. 2026), https://ourtake.bakerbotts.com/post/102mmmi/oregon-sb-1546-the-first-chatbot-law-with-real-teeth.

87. Or. S.B. 1546 § 6 (private right of action; actual or statutory damages of $1,000 per violation; injunctive relief; attorney fees).

88. Wash. H.B. 2225, 69th Leg., 2026 Reg. Sess. (Wash. 2026) (passed Mar. 11, 2026; effective Jan. 1, 2027).

89. See Miller Nash LLP, Oregon's New AI Companion Law: What You Need to Know (Mar. 2026), https://www.millernash.com/industry-news/oregons-new-ai-companion-law-what-you-need-to-know (analyzing applicability ambiguities and customer service exclusion).

90. Wash. H.B. 2225, 69th Leg., 2026 Reg. Sess. (Wash. 2026) (passed Mar. 11, 2026; filed at request of Governor Ferguson; effective Jan. 1, 2027).

91. See Morgan Lewis & Bockius LLP, Washington and Oregon Regulate AI Companions: Key Compliance Changes (Apr. 2026), https://www.morganlewis.com/pubs/2026/04/washington-and-oregon-regulate-ai-companions-key-compliance-changes (comparing disclosure standards across California, Oregon, and Washington statutes).

92. Wash. H.B. 2225 § __ (crisis detection and reporting protocol requirements, including annual public disclosure of number of crisis referral notifications issued).

93. Id. § __ (defining "manipulative engagement techniques" to include mimicking romantic partnership or building romantic bonds, soliciting gift-giving or in-app purchases framed as necessary to maintain the relationship, and encouraging minors to withhold information from trusted adults).

94. See Troutman Pepper Locke LLP, Washington Legislature Passes Consumer-Facing Interactive AI Bill with Private Right of Action (Mar. 2026), https://www.troutmanprivacy.com/2026/03/washington-legislature-passes-consumer-facing-interactive-ai-bill-with-private-right-of-action/ (noting that the bill's broad definition of "AI companion chatbot" could cover commonly used chatbots that recognize users between sessions, subject to the business operations exclusion).

95. Morgan Lewis, supra note 91 (comparing enforcement mechanisms: Oregon provides statutory damages of $1,000 per violation; Washington limits recovery to actual harm but mirrors the My Health My Data Act's private right of action structure).