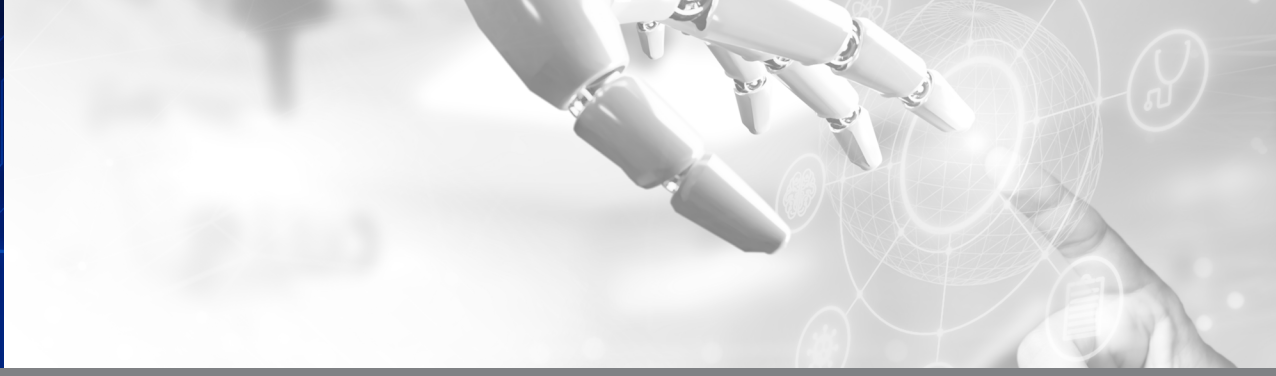

AN ANALYSIS OF

# Relevant State and International AI Regulations and Associated Business Exposures

RT ProExec



# CONTENTS



# CONTACT

For more information, please contact your local RT ProExec broker at rtspecialty.com.



RT ProExec

## EXECUTIVE SUMMARY: NAVIGATING THE AI REGULATORY MAZE

The rapid advancement and widespread adoption of Artificial Intelligence (AI) systems have ushered in a complex and dynamic regulatory environment. Governments worldwide are grappling with how to balance innovation with the imperative to protect individuals and ensure responsible AI deployment. In the United States, the absence of a comprehensive federal framework has led to a growing patchwork of state-level regulations, each addressing specific concerns and risks associated with AI. Concurrently, the European Union's landmark AI Act has emerged as the gold standard, influencing legislative efforts worldwide. This fragmented landscape demands that businesses adopt agile and comprehensive AI governance strategies. The recent legislative developments, particularly the removal of a proposed federal moratorium on state AI regulation, underscore the enduring autonomy of states to legislate in this domain. This analysis dives into certain state and international AI regulations, detailing some of their requirements, compliance strategies, and penalties. It further examines the wide range of exposures and liabilities businesses face when developing or utilizing AI tools, whether internally built or sourced from third parties. Finally, it explores how specialized insurance products, such as Technology Errors & Omissions (E&O) and Cyber & Privacy Liability insurance, can serve as critical financial safeguards against these emerging risks.

## THE EVOLVING LANDSCAPE OF AI REGULATION: FEDERAL CONTEXT AND STATE AUTONOMY

The trajectory of AI regulation in the United States recently experienced a pivotal moment with the "One Big Beautiful Bill Act" (OBBBA). This budget reconciliation bill, passed by the U.S. House of Representatives, initially included a provision for a 10-year moratorium on the enforcement of most state and local laws targeting AI systems. Proponents of this moratorium argued that a single federal standard would reduce compliance burdens for AI developers, thereby fostering innovation and maintaining U.S. competitiveness in the fast-moving AI race. The proposed pause was also seen as a mechanism to streamline AI deployment by eliminating the need to track and implement diverse AI rules across 50 states.

**Governments worldwide are grappling with how to balance innovation with the imperative to protect individuals and ensure responsible AI deployment.**

However, this provision encountered substantial opposition from a wide array of stakeholders. Parent advocates, tech policy think tanks, and state legislators voiced strong concerns, perceiving the moratorium as prioritizing corporate interests over the well-being and safety of children and marginalized online populations. A bipartisan coalition of 40 state attorneys general formally objected, asserting that OBBBA infringed upon state police powers related to health and safety, raising potential issues under the Tenth Amendment. These objections highlighted a tension between federal economic and innovation objectives and state-level public safety and consumer protection priorities.

In a decisive move, the Senate voted 99-1 to remove the AI moratorium provision from the bill. The rationale behind this removal was the conviction that states should retain the authority to enact protective laws until Congress establishes comprehensive, federally preemptive legislation that includes sufficient safeguards.

The removal of the federal AI moratorium solidifies the continuation in the United States of a fragmented, state-led regulatory landscape. States have actively stepped into the regulatory void created by the absence of a federal AI governance legislation. This proactive stance by state legislatures, often referred to as "laboratories of democracy" allows for more agile responses to emerging AI-related harms, such as deepfake abuse and self-harm risks from AI chatbots. Consequently, businesses operating across state lines must contend with a complex and varied set of regulations rather than a streamlined federal standard. This ongoing legislative activity at the state level is expected to continue, with a focus on

consumer protection and harm mitigation, filling the regulatory gaps left by a slower federal legislative process. [1,13, 19, 20, 25]

## KEY STATE-LEVEL AI REGULATIONS IN THE U.S.

The following section provides an overview of some of the significant AI regulations enacted at the state level in the U.S., including their effective dates, certain specific requirements, compliance strategies, and penalties. This list provides only a sample and is not exhaustive.

## COLORADO AI ACT (CAIA)

The Colorado Artificial Intelligence Act (CAIA) is set to become effective on February 1, 2026. This legislation adopts a risk-based approach to AI regulation, drawing parallels with the European Union's AI Act, and primarily focuses on "high-risk" AI systems. A high-risk AI system is defined as one that, when deployed, "makes, or is a substantial factor in making a consequential decision" that has a material legal or similarly significant effect on a consumer's access to or cost of essential services. A central concern of the CAIA is "algorithmic discrimination," which refers to unlawful differential treatment or impact that disfavors individuals.

The CAIA imposes distinct duties on both developers and deployers of high-risk AI systems. Developers are mandated to exercise "reasonable care" to prevent algorithmic discrimination. This includes providing deployers with a general statement outlining the system's intended uses and detailed documentation on how known or foreseeable risks of algorithmic discrimination are managed. Developers must also publicly disclose their high-risk AI systems and their risk management practices on their website or in a public inventory. A critical reporting requirement dictates that if a developer discovers, or learns from a credible source, that their high-risk AI system has caused or is likely to cause algorithmic discrimination, they must inform the Colorado Attorney General and all known deployers within 90 days. Deployers, which include employers, similarly bear the responsibility of exercising "reasonable care" to protect consumers from algorithmic discrimination. Before a high-risk AI system is used to make a consequential decision about a consumer, deployers must provide notification detailing the system's purpose and the nature of the decision. In cases of adverse decisions, deployers are required to furnish reasons for the decision, the AI's contribution, the type of data processed, and offer the consumer an opportunity to correct inaccurate personal data and appeal the decision, with human review where technically feasible. Public transparency is also a key mandate, requiring deployers to clearly and readily make available on their website information about the types of high-risk AI systems deployed, their methods for managing discrimination risks, and the nature and source of collected data. Annual impact assessments are also required for high-risk AI systems, or within 90 days of substantial modification, to analyze discrimination risks and mitigation steps. Like developers, deployers must also notify the Attorney General of any discovered algorithmic discrimination within 90 days.

**Businesses should establish detailed internal processes for identifying and reporting algorithmic discrimination to the Attorney General.**

To comply with the CAIA, businesses should consider implementing iterative risk management policies and programs, ideally aligning with frameworks published by the Colorado Attorney General or national/international standards such as NIST's AI Risk Management Framework. Conducting annual impact assessments that scrutinize algorithmic discrimination risks and mitigation efforts aide in compliance. Developing clear procedures for consumer notifications regarding high-risk AI use and adverse decisions is also critical. Businesses should consider establishing detailed internal processes for identifying and reporting algorithmic discrimination to the Attorney General. A proactive step for employers is to inventory their AI uses, particularly in human resources practices, to determine if they fall under the definition of high-risk AI systems and assess their compliance needs.

The Colorado Attorney General holds exclusive enforcement authority for the CAIA. Violations of the AI Act, such as failing to prevent algorithmic discrimination in high-risk AI systems, neglecting required impact assessments, or not updating assessments within 90 days of a substantive modification, incur a fine of up to $20,000 per violation.

Violations of the Act are deemed a deceptive trade practice under Colorado's Consumer Protection Act (CCPA). If AI related deceptive trade practices are committed against an elderly person, the fine increases to up to $50,000. While the CAIA itself does not explicitly authorize private rights of action, the classification as a deceptive trade practice introduces an element of ambiguity, as CCPA generally allows for private rights of action. This legal interpretation could potentially open avenues for individual or class action lawsuits, despite the Act's stated enforcement mechanism.


The law provides potential affirmative defenses in enforcement actions if a deployer or employer discovers and cures a violation through feedback, "adversarial testing or red teaming," or an internal review process, and is otherwise in compliance with NIST's Artificial Intelligence Risk Management Framework or another equivalent internationally recognized framework. This provision creates a clear incentive structure, indicating that proactive, documented AI governance is not merely a best practice but can serve as a significant legal shield against enforcement actions.

The Colorado AI Act is widely viewed as a template for future state AI regulation. States like Connecticut, Massachusetts, New Mexico, New York, and Virginia are considering bills that largely mirror the CAIA's approach, particularly in imposing safeguards against bias by AI systems. This suggests that the detailed requirements for developers and deployers, especially concerning risk management, impact assessments, and algorithmic discrimination, are likely to become standard elements across other state legislative efforts. For businesses operating nationally, this implies a growing convergence in regulatory expectations, even if specific details may vary by jurisdiction. [5, 7, 8, 26]

## UTAH ARTIFICIAL INTELLIGENCE POLICY ACT

The Utah Artificial Intelligence Policy Act became effective on May 1, 2024. This Act distinguishes itself as the first U.S. state law to impose specific transparency obligations on companies using generative artificial intelligence (Gen AI). Its scope extended to businesses governed by Utah's consumer protection legislation and those operating in regulated professions, such as medicine and accounting.

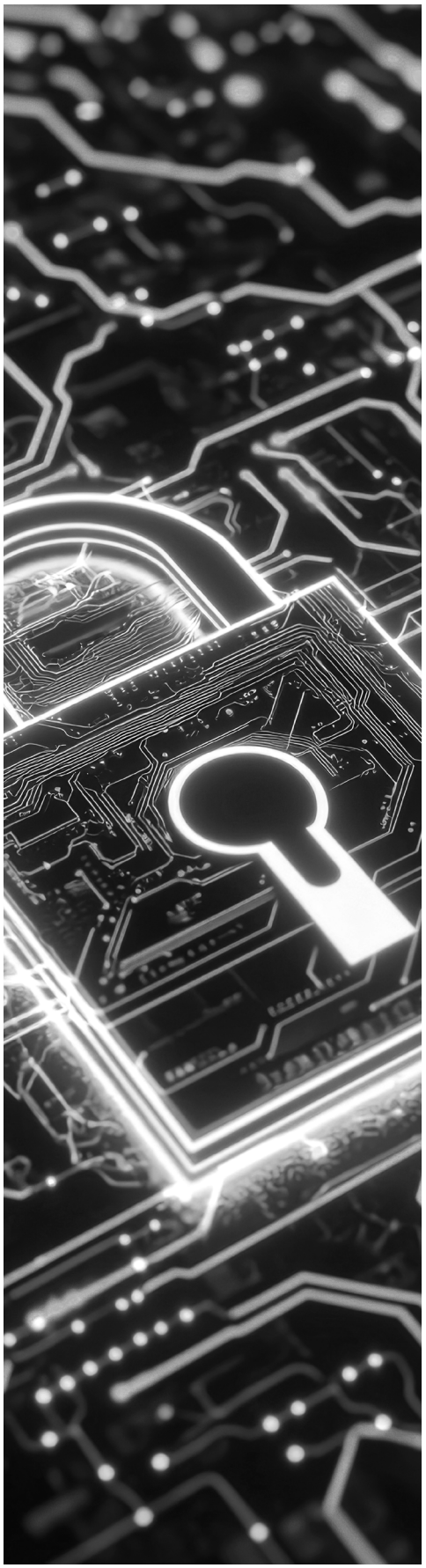
**The Utah Artificial Intelligence Policy Act became effective on May 1, 2024. This Act distinguishes itself as the first U.S. state law to impose specific transparency obligations on companies using generative artificial intelligence (Gen AI).**

The Act established a two-tiered disclosure requirement for generative AI use. For organizations under general consumer protection legislation, disclosure of generative AI use is mandated if a user questions whether they are interacting with AI instead of a human. In such instances, the business must provide a clear and obvious disclosure verifying the use of AI. For generative AI employed in regulated professions, the Act requires proactive and obvious notification at the beginning of the contact. This means that if the communication is verbal, the disclosure must occur at the outset of the discussion; for textual electronic exchanges, the AI system must introduce itself before any substantive conversation begins.

In late March 2025, Utah enacted further legislation amending various aspects of the UAIPA ). The amendments, which became effective on May 7, 2025, include extension of the UAIPA's repeal date from May 2025 to July 2027 and clarification that the UAIPA does not displace any other remedy or right authorized under state or federal laws. The amendments also narrow the scope of the UAIPA's disclosure obligations and establish a new enforcement safe harbor. The disclosure requirement is now limited to "high-risk" AI. "High-risk artificial intelligence interaction" means an interaction with generative artificial intelligence that involves (a) the collection of sensitive personal information, (b) the provision of personalized recommendations, advice, or information that could reasonably be relied upon to make significant personal decisions, or (c) other applications as defined by division rule.

Compliance with the Utah AI Act necessitates that businesses involved in high-risk interactions thoroughly understand the definitions of "generative artificial intelligence" and "artificial intelligence" as outlined in the Act. Implementing systems capable of detecting when a user questions AI interaction and subsequently providing immediate, clear disclosures may be needed for compliance. For businesses in regulated professions, integrating proactive and obvious AI disclosures into all initial contacts, whether verbal or textual, may be needed. Businesses may consider engaging with the Office of Artificial Intelligence Policy and the AI Learning Laboratory Program. This program offers a regulatory sandbox for testing AI technologies, potentially providing modest exemptions from certain state rules during participation, balancing innovation with controlled oversight.

The Utah Division of Consumer Protection is responsible for enforcing the Act. Penalties for non-compliance include administrative fines of up to $2,500 per violation. Violations of court or administrative orders related to the Act can result in more substantial fines, reaching up to $5,000 per breach. The Act also introduces criminal liability under Section 76-2-107 of Utah's criminal code for individuals who use or direct generative AI to commit or participate in illegal activities, preventing the evasion of legal responsibility by attributing criminal actions to AI systems.



Utah's specific focus on generative AI transparency, particularly the requirement for disclosure for high-risk AI interactions when a user questions AI interaction or proactively in regulated professions, directly addresses the increasing blurring of lines between human and AI communication. This emphasis signals a broader trend in state regulation to govern not just the outputs of AI, but also the nature of the interaction with AI systems, especially as generative AI becomes more sophisticated and indistinguishable from human interaction. The establishment of the AI Learning Laboratory Program and the potential for regulatory mitigation agreements offering exemptions for testing new AI technologies indicate a strategic approach by Utah to balance innovation with regulatory oversight. [5, 24, 26, 31]

## CALIFORNIA AI TRANSPARENCY ACT (SB 942) AND OTHER KEY CA LAWS

California's legislative efforts in AI regulation are comprehensive, with the California AI Transparency Act (SB 942) set to take effect on January 1, 2026. SB 942 primarily targets "Covered Providers," defined as entities that create or produce a Generative AI system with over 1,000,000 monthly users and is publicly accessible in California. The Act's requirements specifically apply to image, video, or audio content, but not text.

Key requirements under SB 942 include mandating Covered Providers to make available a free, publicly accessible AI detection tool. This tool must enable users to verify if content was AI-generated, return available provenance data (excluding personal data), and support various content formats. Providers are also obligated to collect ongoing user feedback regarding the tool and implement relevant improvements.

**A significant aspect of SB 942 involves contractual obligations for licensees. If a GenAI system is licensed to a third party, the provider must contractually ensure that licensees maintain the latent disclosure capabilities.**

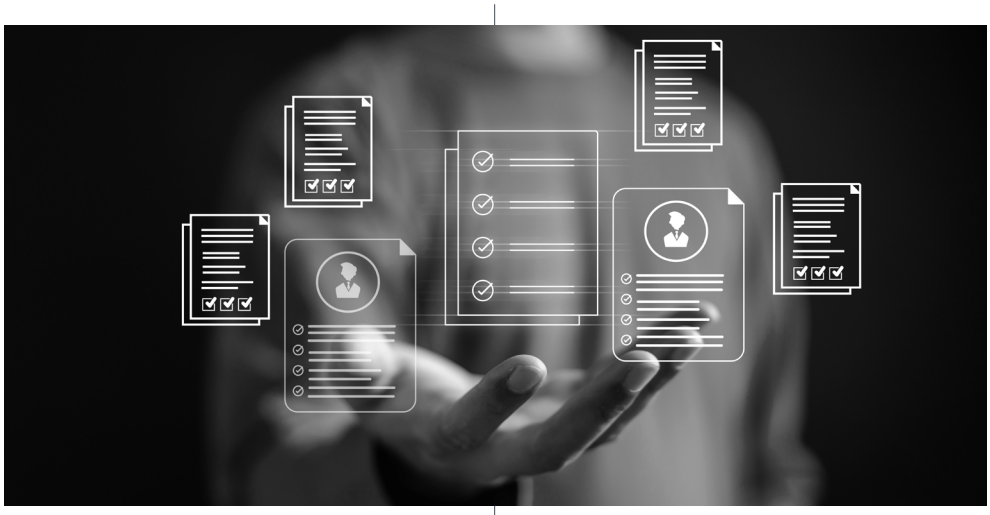
AI-generated content must also incorporate specific disclosures.

"Latent" (hidden) disclosures must be embedded permanently within the content, containing the provider's name, AI system details, creation time and date, and a unique identifier, all detectable by the provider's AI detection tool. Providers must also offer users the option to include "manifest" (visible) disclosures, clearly indicating the AI origin of the content and designed to be difficult to remove.

A significant aspect of SB 942 involves contractual obligations for licensees. If a GenAI system is licensed to a third party, the provider must contractually ensure that licensees maintain the latent disclosure capabilities. Should a provider discover that a licensee has altered a licensed GenAI system to no longer include the required latent disclosures, the license must be revoked within 96 hours.

To enable compliance with SB 942, businesses may need to develop or procure a compliant AI detection tool and ensure its public accessibility. Implementing technical mechanisms to embed permanent latent disclosures in all AI-generated image, video, and audio content may be needed, as is providing users with a clear option for manifest disclosures. Businesses should also consider reviewing and updating all GenAI license agreements to explicitly include contractual obligations for licensees to maintain latent disclosure capabilities and grant the provider the right to revoke licenses within 96 hours if these capabilities are compromised. Establishing internal monitoring processes to ensure licensee compliance with disclosure requirements may be advisable.

Penalties for non-compliance can be substantial, with businesses facing fines of up to $5,000 for each day of violation. If a licensee fails to cease using a GenAI system within 96 hours after license revocation, a civil action for injunctive relief and reasonable attorney fees may be brought against the licensee.



Beyond SB 942, California has enacted several other targeted AI laws, primarily effective January 1, 2025:

- AB 1831 expands the scope of existing child pornography laws to include content that is digitally altered or generated by AI systems.
- SB 926 criminalizes the creation and distribution of non-consensual deepfake pornography, granting victims a private right of action to sue for damages.
- SB 981 mandates social media platforms in California to establish reporting tools for sexually explicit digital identity theft, requiring temporary content hiding, report confirmation within 48 hours, and status updates within seven days.
- AB 2602 protects individuals from unauthorized use of their digital replicas in personal or professional service contracts, making certain provisions unenforceable if they lack specific usage descriptions or legal representation.
- AB 1836 restricts the commercial use of deceased personalities' digital replicas without prior consent from their estate, with civil liability for violators.

California's legislative approach, particularly SB 942's emphasis on AI detection tools and latent/manifest disclosures, directly addresses the growing concern over AI-generated synthetic content and deepfakes. This focus, reinforced by the suite of other California laws criminalizing deepfake pornography and mandating labeling for deceptive election content, demonstrates a strong commitment to combating misinformation and unauthorized use of likeness and voice enabled by generative AI.

Additionally, SB 942's requirement for contractual obligations for licensees to maintain clear disclosure capabilities introduces a significant element of supply chain risk. This means that the original provider of a GenAI system retains a degree of responsibility for the traceability and authenticity of AI-generated content, even when the system is licensed to third parties. Businesses relying on external AI solutions must evaluate their contracts to determine if they reflect these requirements, and providers must consider implementing detailed technical and contractual mechanisms to help manage extended liability across the AI supply chain. [5, 6, 17]

## TEXAS RESPONSIBLE AI GOVERNANCE ACT (TRAIGA)

The Texas Responsible AI Governance Act (TRAIGA) is scheduled to take effect on January 1, 2026. Although initially conceived as a broad regulatory proposal, TRAIGA was scaled back during the legislative process but still introduces significant compliance requirements for both businesses and government entities in Texas. The Act primarily focuses on preventing discriminatory, harmful, and manipulative uses of AI.

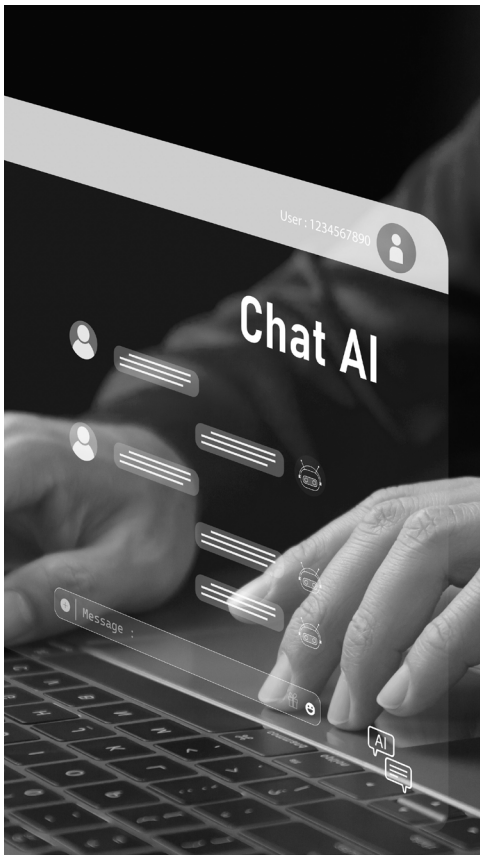
TRAIGA imposes categorical restrictions on the development and deployment of AI systems for specific prohibited purposes.

**TRAIGA imposes categorical restrictions on the development and deployment of AI systems for specific prohibited purposes.**

These include behavioral manipulation, discrimination, the creation or distribution of child pornography or unlawful deepfakes, and the infringement of constitutional rights. The Act also includes stricter requirements for public entities, such as enhanced transparency and the necessity of biometric data consent. To foster responsible innovation, TRAIGA establishes a regulatory sandbox program for developers, allowing them to test and develop AI systems for up to 36 months under a waiver of certain state regulatory requirements, provided they submit detailed descriptions, benefit assessments, and mitigation plans. Additionally, the Act creates the Texas Artificial Intelligence Advisory Council, tasked with providing guidance on future AI policy.

For compliance, developers and deployers operating in Texas should consider proactively establishing an internal process designed to identify and prevent potential violations, including the implementation of recognized best practices such as NIST's AI Risk Management Framework. Businesses may need to evaluate AI systems to ensure that their AI systems are not utilized for any of the explicitly prohibited purposes. For interactions involving the public sector, adherence to enhanced transparency and consent requirements may be needed. Participation in the regulatory sandbox program may be a valuable strategy for businesses developing new AI systems, offering a controlled environment for testing and development.

Enforcement of TRAIGA falls under the purview of the Texas Attorney General. Upon receiving a notice of violation, a party is granted a 60-day period to cure the alleged violation and provide supporting documentation. Uncured violations are subject to substantial fines ranging from $80,000 to $200,000 per violation. Furthermore, state agencies are empowered




to sanction licensed parties found liable for TRAIGA violations, with potential actions including suspending or revoking licenses and imposing monetary penalties of up to $100,000.

TRAIGA's broad categorical prohibitions against harmful AI applications, such as behavioral manipulation and discrimination, signal a strong regulatory stance against the misuse of AI. The Act's dual focus on regulating both private sector use and imposing stricter requirements for public entities demonstrates a nuanced approach to governing AI deployment within governmental operations, setting a standard for responsible public sector AI. Similar to Colorado, TRAIGA incentivizes proactive risk management by encouraging the implementation of strong internal processes, including adherence to frameworks like NIST's AI Risk Management Framework. This approach makes it clear that formal AI governance programs are not just recommended but may become a critical business necessity to help mitigate severe penalties and demonstrate due diligence. [22, 23]

**To comply with the Ensuring Likeness, Voice, and Image Security (ELVIS) Act, businesses must secure proper licenses for the use of digital replicas, voice clones, or any AI-generated content that incorporates an individual's name, photograph, voice, or likeness.**

## TENNESSEE ELVIS ACT (ENSURING LIKENESS, VOICE, AND IMAGE SECURITY ACT)

The Tennessee Ensuring Likeness, Voice, and Image Security (ELVIS) Act, which became effective on July 1, 2024, significantly expands the state's right of publicity laws, directly addressing the challenges posed by artificial intelligence. This pioneering legislation makes Tennessee the first state to comprehensively regulate the unauthorized commercial use of voices through AI.

The ELVIS Act establishes a property right in an individual's name, photograph, voice, or likeness, making these rights freely assignable and licensable. A violation occurs when an individual's identity is used for advertising, merchandise, or fundraising purposes without authorization. The Act extends this protection to digital replicas and voice clones, explicitly covering instances where a person publishes, performs, distributes, transmits, or otherwise makes available to the public an individual's voice or likeness with knowledge that such use was unauthorized. It also applies if a person distributes or makes available technology whose primary purpose or function is to create such unauthorized uses. The Act provides for postmortem rights, lasting for ten years after death and potentially renewable indefinitely if commercial exploitation continues at least once every two years.

To comply with the ELVIS Act, businesses should consider reviewing to determine if they have proper licenses for the use of digital replicas, voice clones, or any AI-generated content that incorporates an individual's name, photograph, voice, or likeness. A thorough understanding of the Act's broad scope of "commercial use" is essential. In addition, developers and distributors of AI tools must consider an evaluation of their technologies to determine if they are primarily designed or knowingly used for unauthorized replication of voices or likenesses.

The Act introduces enforcement capabilities, offering civil remedies such as injunctive relief, actual damages, and treble damages for willful violations. It also provides for criminal penalties for unauthorized commercial use. A particularly significant aspect of the ELVIS Act is its imposition of liability on technology providers. This means that developers or distributors who knowingly provide AI tools primarily designed for unauthorized voice replication can be held accountable, extending liability beyond the direct user and emphasizing the responsibility of those who create the underlying AI technology. This pioneering protection for voice and likeness is a direct response to generative AI's ability to create highly realistic deepfakes, establishing a new boundary in intellectual property and publicity rights protection. The inclusion of extended liability for AI tool providers is a critical development for AI developers, as it expands the scope of accountability within the AI supply chain. [14, 21]

## STATES WITH AI LEGISLATION IN PROGRESS

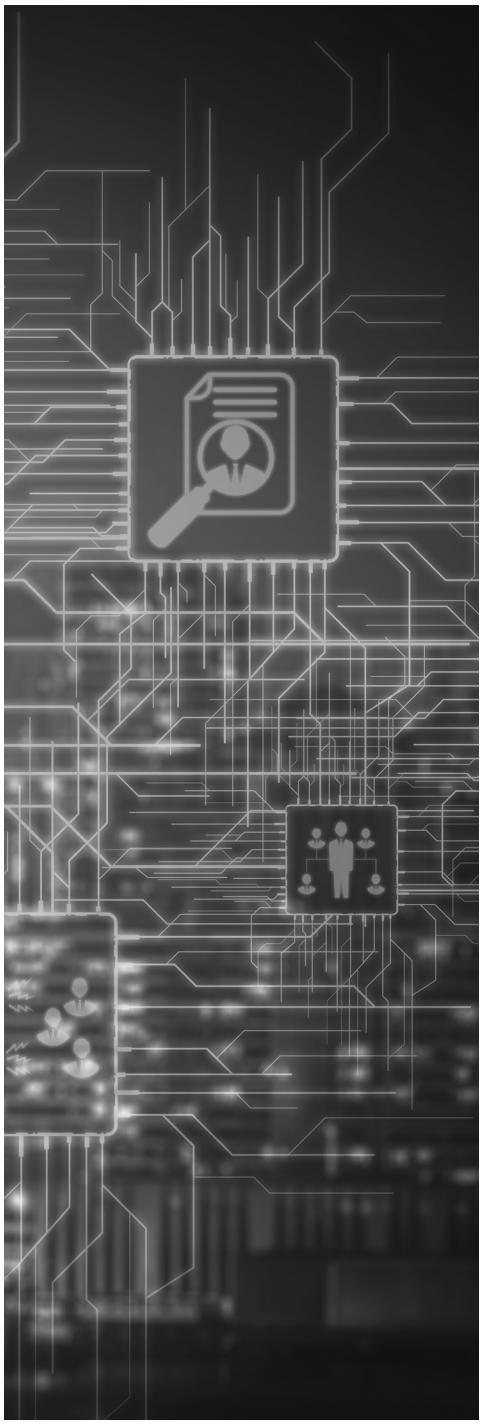
The legislative activity surrounding AI is not limited to the states that have already enacted laws. Several other states are actively considering their own AI legislation, often drawing inspiration from existing frameworks. For instance, state legislatures in Massachusetts, New Mexico, New York, and Virginia are considering bills that generally track the Colorado AI Act's approach, particularly in imposing safeguards against bias by AI systems.

## THE EUROPEAN UNION'S AI ACT: A LEADING BENCHMARK

The European Union's Artificial Intelligence Act (EU AI Act), formally Regulation (EU) 2024/1689, represents the world's first comprehensive legal framework for AI systems. It officially entered into force on August 1, 2024, though its prohibitions and

# AN ANALYSIS OF RELEVANT STATE AND INTERNATIONAL AI REGULATIONS AND ASSOCIATED BUSINESS EXPOSURES

**The EU AI Act's comprehensive, risk-based approach positions it as a leading benchmark for AI regulation, influencing legislative efforts worldwide and requiring multinational corporations to align their AI governance practices accordingly.**



obligations will be phased in over several years, acknowledging the complexity of AI systems and allowing businesses time to adapt.

The implementation timeline for the EU AI Act is structured as follows:

- **February 2025:** Prohibitions on certain "unacceptable risk" AI systems become applicable. These include AI systems that involve social scoring, subliminal manipulation, or biometric categorization in workplaces, which are deemed a threat to fundamental rights. Companies must also begin training staff on AI literacy.
- **May 2025:** Application of codes of practice for General Purpose AI (GPAI) systems begins.
- **August 2025:** Obligations for providers of General Purpose AI models go into effect. Member states must appoint competent authorities to oversee the Act, and the European Commission will conduct an annual review of the list of prohibited AI practices. Providers must disclose details about their AI models, including training data and safety measures.
- **February 2026:** Post-market monitoring requirements will be implemented.
- **August 2026:** Comprehensive obligations for "high-risk" AI applications become fully enforceable. This includes requirements for detailed documentation, human oversight, data quality, and transparency measures.
- **August 2027:** Enforcement extends to existing high-risk AI systems embedded in products (medical devices, toys, etc.) already regulated by other EU safety legislation. Providers of general-purpose AI models that entered the market prior to August 2025 must also be fully compliant.
- **December 2030:** The final compliance deadline for AI systems integrated within large-scale IT infrastructure that entered the market before August 2027.

Central to the EU AI Act is its risk-based approach, categorizing AI systems based on the level of risk they present: unacceptable, high, limited, and low risk. Systems posing "unacceptable risk" are strictly prohibited, as they are considered a clear threat to safety and fundamental rights.

For "high-risk" AI systems, those with the potential to significantly impact individuals' safety, health, or rights (in critical infrastructure, education, employment, law enforcement, healthcare, credit scoring), the Act imposes stringent requirements. Providers of such systems must ensure vigorous data governance practices, including detailed documentation of datasets, processes for reducing potential bias, and transparency regarding functionality and limitations. Human oversight is mandated, emphasizing accountability and control. High-risk systems require thorough pre-market testing, a comprehensive risk management system, and continuous post-deployment monitoring. They must undergo conformity assessments, which can be internal or by approved third-party bodies, to prove compliance before being placed on the market, and must bear a CE marking. These systems also need to be registered in an EU database.

The Act also specifically addresses General-Purpose AI (GPAI) models, such as large language models. Developers of GPAI models must disclose extensive documentation about training data, risk management strategies, and safeguards against misuse. This includes providing information for downstream providers, implementing policies to comply with EU copyright laws, and offering detailed summaries of the content used for training. Open-source models face fewer obligations unless their scale or application generates significant systemic risks.

Transparency obligations extend to requiring AI providers to mark synthetic content like deepfakes as artificially generated and to inform users when AI systems analyze emotions or categorize people by physical traits (with exceptions for legal uses). The Act emphasizes transparency and responsible data governance, closely aligning its requirements with existing frameworks like the General Data Protection Regulation (GDPR), mandating clear documentation of data usage, rigorous

access control, and strong cybersecurity and privacy protections. Regulatory sandboxes are also encouraged to facilitate safe testing of AI technologies.

Non-compliance with the EU AI Act carries significant penalties, with fines potentially reaching up to €35 million or 7% of an entity's global annual turnover, whichever is greater. These substantial penalties underscore the critical importance of early preparation and adherence to the Act's provisions.

The EU AI Act's comprehensive, risk-based approach positions it as a leading benchmark for AI regulation, influencing legislative efforts worldwide and requiring multinational corporations to align their AI governance practices accordingly. The multi-year phased implementation acknowledges the inherent complexity of AI systems, providing businesses with a structured timeline to adapt their operations and ensure compliance. However, this extended timeline also highlights the critical need for early preparation, given the severity of the potential penalties for non-compliance. [3, 10, 11, 12, 18]

## BUSINESS EXPOSURES AND LIABILITIES FROM AI ADOPTION

Businesses are increasingly integrating AI tools into various facets of their operations, whether by building proprietary AI systems or by utilizing third-party AI solutions. This widespread adoption, while offering significant benefits, at the same time introduces a complex array of legal and operational exposures. The evolving regulatory landscape, coupled with established legal principles, may create substantial liability risks for organizations.

One of the most significant legal risks is data privacy violations. AI tools often rely on vast datasets, which frequently include personal, financial, or health-related information. Mishandling this data can lead to severe penalties under comprehensive privacy laws like the EU's GDPR, the California Consumer Privacy Act (CCPA), or sector-specific federal regulations such as HIPAA (for health data) and the Gramm-Leach-Bliley Act (for financial data). Risks include data breaches or improper storage of personal data, failing to obtain adequate user consent for data collection or use, and a lack of transparency regarding how customer data is processed by AI tools. New York's SHIELD Act, for instance, mandates reasonable data security safeguards, which will apply to AI systems handling sensitive information.

Intellectual property (IP) issues pose another substantial threat. AI tools may be trained on copyrighted material without proper permission, or they may generate new content (text, images, audio) with unclear ownership rights. This can lead to claims of copyright infringement or misappropriation. The lack of clear legal frameworks regarding IP ownership for AI-generated content can result in disputes, and sharing too much information with AI systems could even jeopardize future patent applications. Businesses must confirm ownership rights and secure proper licenses for any copyrighted material used by or within their AI systems.

**One of the most significant legal risks is data privacy violations. AI tools often rely on vast datasets, which frequently include personal, financial, or health-related information.**

The risk of bias and discrimination is a pervasive concern. AI algorithms, if trained on biased or unrepresentative data, can produce discriminatory outcomes, particularly in critical areas such as hiring, lending, credit decisions, and customer service. Such biased decisions can lead to legal challenges under anti-discrimination laws. Regulatory bodies and courts increasingly expect companies to ensure fairness, and reliance on technology, including AI, is not a defense against liability for discrimination. Routine audits and the careful selection of training data are essential to mitigate this risk.

Liability for AI decisions and errors is a growing area of concern. If an AI tool makes a mistake, such as approving a fraudulent transaction, providing inaccurate information, or even causing physical harm (autonomous vehicles or medical devices), the business deploying or developing it can be held responsible. This can fall under product liability laws, negligence claims, or other torts. Determining fault can be complex, often involving multiple parties including manufacturers, software developers, operators, and end-users. Common law principles extend to AI, holding companies liable for their AI systems' actions much as they would be liable for their human employees. This means businesses are expected to supervise their AI systems as they would their human workforce, and even if an AI tool is acquired from a vendor or used independently by an employee, the business may bear primary legal responsibility for issues that arise.

Consumer protection and misrepresentation claims can arise if AI-powered tools, especially those used in marketing or customer interactions (like chatbots), make misleading claims about products or services, or fail to clearly disclose the use of AI. This can violate false advertising and deceptive practices laws.

The use of third-party AI tools introduces additional layers of risk and complexity, forming a critical aspect of supply chain liability. While businesses may outsource AI capabilities, they do not necessarily outsource their legal liability. Without clear agreements, businesses might lose control or ownership of their data, or face claims of IP infringement originating from the third-party tool. Thorough vendor due diligence is important, ensuring that third-party providers comply with all relevant laws, regulations, and ethical standards. Contractual provisions, such as indemnification clauses, can help shift legal liability for issues like copyright infringement back to the AI provider, where appropriate. However, even with such clauses, the primary user of the AI system may still face initial legal action and reputational damage.

Finally, the increasing use of AI by regulatory enforcement agencies (SEC identifying suspicious filings, EPA targeting inspections) means that businesses can face enforcement actions if they fail to

demonstrate adequate governance of their AI systems. For instance, a firm might face regulatory scrutiny if it cannot explain how its AI models make decisions or if it fails to monitor their outputs effectively.

The various risks associated with AI are often interconnected. For example, biased training data (IP risk) can lead to discriminatory hiring decisions (bias risk), resulting in regulatory enforcement actions (regulatory risk) and potential lawsuits (liability risk). This interconnectedness can make a holistic risk management approach beneficial, helping to ensure that AI policies cover acceptable uses, data quality, human oversight, and clear communication about AI's role and limitations. [2,15, 16, 27, 28, 30]

## MITIGATING AI EXPOSURES: THE ROLE OF INSURANCE

As businesses navigate the complex landscape of AI-related liabilities, specialized insurance products, particularly Technology Errors & Omissions (E&O) and Cyber & Privacy Liability insurance, may become useful tools for risk mitigation.

## TECHNOLOGY E&O INSURANCE

Technology E&O insurance is designed to protect technology companies from professional liability and errors or omissions in the delivery of their products and services. Coverage will, in many instances, extend to liabilities tied to the use, development, or outputs of Artificial Intelligence.

Common examples of risk typically covered under a Technology E&O policy, especially when tailored to AI use cases, include:

- **Algorithmic decision errors:** Such as those occurring in hiring, lending, or other automated services.
- **Copyright claims:** Arising from AI-generated content.
- **Regulatory actions:** Stemming from automated services or AI-related non-compliance.
- **Training data misuse:** Including issues related to data privacy or intellectual property.
- **Model hallucinations or consumer misguidance:** Where AI provides inaccurate or misleading information.

Insurance agents and brokers must carefully review policy language, as common exclusions can limit coverage. Some examples of typical exclusions include. intentional wrongdoing, certain regulatory violations, and bodily injury or property damage (typically covered under General Liability). A critical consideration in the evolving AI insurance market is the debate around affirmative AI endorsements versus silent AI coverage. While affirmative endorsements explicitly grant coverage for AI-related liabilities, they can limit coverage if the listed AI perils are narrowly defined, potentially excluding claims that do not fit within the specified categories. Conversely, silent AI coverage, when paired with broad definitions of professional services and no explicit exclusions, may offer greater flexibility and better defense positioning, especially for rapidly evolving or experimental AI platforms, as it avoids narrowing coverage to pre-defined AI use cases. Navigating these nuances requires careful policy review and, often, expert consultation to help select a policy. [29]

## CYBER & PRIVACY LIABILITY INSURANCE

Cyber & Privacy Liability insurance is often a complement to Technology E&O, particularly given AI's inherent reliance on large datasets and its potential to trigger data privacy violations. This coverage typically directly addresses the financial consequences of cyber incidents and privacy breaches.

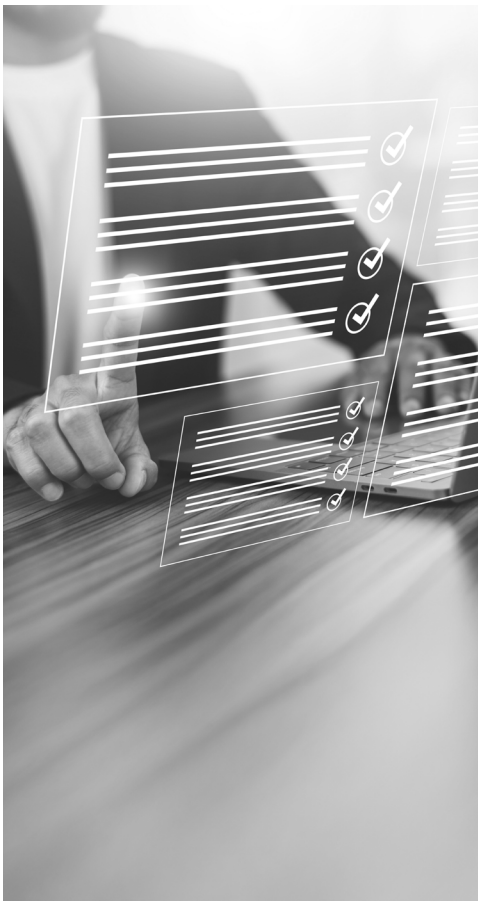
Key coverages typically include:

- **First-party coverage:** Protection for the insured's own business assets, such as data restoration costs, business interruption losses resulting from a cyber security incident, ransomware, business interruption, and system failure.
- **Third-party coverage:** Protection against claims from clients or other third parties affected by a cyber security incident, including liabilities arising from data breaches, network security failures, privacy violations, and regulatory proceedings or Payment Card Industry (PCI) investigations.

The benefits of Cyber & Privacy Liability insurance are extensive. It provides crucial support for breach response processes, access to resources, helping to minimize damage, manage regulatory compliance obligations, and protect the company's reputation following an incident. This coverage is beneficial for meeting contractual obligations, as many clients and partners now require evidence of cyber liability coverage.

Given the data-intensive nature of AI systems, cyber and privacy liability insurance is often beneficial. AI's reliance on vast amounts of data, often including sensitive personal information, making data privacy violations a primary risk for most businesses. This insurance is designed to

**Insurance agents and brokers must carefully review policy language, as common exclusions can limit coverage.**



help address the financial and reputational consequences of such breaches, providing a critical layer of protection to help mitigate losses from the most common and potentially devastating AI related exposure.

## CONCLUSION AND RECOMMENDATIONS

The regulatory landscape surrounding Artificial Intelligence is rapidly evolving, characterized by a dynamic interplay between federal considerations and assertive state-level initiatives in the United States, alongside the international framework established by the European Union. The decisive removal of the proposed federal AI moratorium has cemented a fragmented, state-led approach in the U.S., compelling businesses to navigate a complex and diverse set of compliance obligations. This environment underscores the agility of states in addressing specific harms like algorithmic discrimination, deepfakes, and unauthorized digital replicas, often prioritizing consumer protection and public safety. The EU AI Act, with its comprehensive, risk-based methodology and phased implementation, serves as a significant benchmark, requiring compliance from any entity operating within or offering AI systems to the EU market.

**The adoption of AI tools, whether developed internally or sourced from third parties, exposes businesses to a multifaceted array of legal and operational liabilities.**

The adoption of AI tools, whether developed internally or sourced from third parties, exposes businesses to a multifaceted array of legal and operational liabilities. These include pervasive risks related to data privacy violations, intellectual property infringement, algorithmic bias and discrimination, direct liability for AI decisions and errors, consumer protection concerns, and complex supply chain risks when utilizing third-party AI solutions. The principle that companies are responsible for the actions of their AI systems, akin to their human workforce, drives this legal landscape, demanding strong supervision and clear internal policies. The interconnected nature of these risks means that a single AI deployment can trigger multiple legal exposures, making a complete risk management strategy beneficial.

To navigate this intricate regulatory and liability environment, businesses are advised to consider implementing several. strategic measures:

- **Proactive AI Governance:** Establish and continuously update comprehensive AI governance frameworks and policies. This includes defining acceptable uses of AI, ensuring data quality, implementing risk management systems, and mandating human oversight for critical AI-driven decisions. Adherence to internationally recognized frameworks, such as NIST's AI Risk Management Framework, can provide a structured approach to demonstrating "reasonable care" and may serve as an affirmative defense in enforcement actions.
- **Continuous Regulatory Monitoring:** Given the rapid pace of legislative developments, businesses must continuously monitor new and evolving AI laws at both state and international levels. This includes tracking specific requirements, effective dates, and enforcement mechanisms to ensure timely adaptation of compliance strategies.
- **Vendor Management:** For businesses adopting third-party AI tools, thorough due diligence on vendors is critical. Contractual agreements must clearly define responsibilities, address data ownership, include indemnification clauses for potential liabilities (IP infringement), and ensure that third-party providers adhere to all relevant legal and ethical standards.
- **Strategic Insurance Procurement:** Review and strategically secure insurance coverage. Carefully consider "affirmative" versus "silent" AI coverage to help ensure broad protection. Consider whether tailored or specialized coverage is needed. Technology E&O insurance and Cyber & Privacy Liability insurance can play a role in helping to mitigate the financial and reputational consequences of data breaches, privacy violations and the use of AI tools. Policy language should be meticulously reviewed to enable a full understanding of exclusions or limitations on AI-related risks.

By adopting a proactive, comprehensive, and adaptable approach to AI governance and risk management, businesses can better navigate the complexities of the evolving AI regulatory landscape, mitigate potential liabilities, and foster responsible innovation.

## References


[1] AI Regulations Provision Removed from Big Beautiful Bill. (2025, July 2). The 19th News. https://19thnews.org/2025/07/ai-regulations-provision-removed-big-beautiful-bill/

[2] AI Regulatory Enforcement Actions Examples. (2024, December 9). Administrative Conference of the United States. https://www.acus.gov/sites/default/files/documents/AI-Reg-Enforcement-Final-Report-2024.12.09.pdf

[3] AI Regulation in Financial Services: FCA Developments and Emerging Enforcement Risks. (2025, July 1). Regulation Tomorrow. https://www.regulationtomorrow.com/eu/ai-regulation-in-financial-services-fca-developments-and-emerging-enforcement-risks/

[4] AN ACT CONCERNING ARTIFICIAL INTELLIGENCE. (2025, April 9). Connecticut General Assembly. https://www.cga.ct.gov/2025/ba/pdf/2025SB-00002-R000603-BA.pdf

[5] AI Watch: Global Regulatory Tracker - United States. (n.d.). White & Case LLP. https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states

[6] California AI Laws. (n.d.). Pillsbury Winthrop Shaw Pittman LLP. https://www.pillsburylaw.com/en/news-and-insights/california-ai-laws.html

[7] Colorado's Artificial Intelligence Act: What Employers Need to Know. (2024, May 20). Ogletree Deakins. https://ogletree.com/insights-resources/blog-posts/colorados-artificial-intelligence-act-what-employers-need-to-know/

[8] Colorado's Landmark AI Act. (2024, June 20). Skadden, Arps, Slate, Meagher & Flom LLP. https://www.skadden.com/insights/publications/2024/06/colorados-landmark-ai-act

[9] Connecticut Senate approves AI bill. (2024, April 25). International Association of Privacy Professionals (IAPP). https://iapp.org/news/b/connecticut-senate-approves-ai-bill

[10] Countdown to Compliance: Essential EU AI Act Milestones. (2025, May 8). CCB Journal. https://ccbjournal.com/articles/key-dates-to-know-when-eu-ai-act-compliance-gets-real

[11] EU AI Act Guide: Compliance Steps for Your Business. (n.d.). Institute of AI Studies. https://www.instituteofaistudies.com/insights/the-eu-ai-act-is-here-an-explanation-for-business-compliance

[12] EU AI Act Implementation Timeline. (2024, October 1). Goodwin Procter LLP. https://www.goodwinlaw.com/en/insights/publications/2024/10/insights-technology-aiml-eu-ai-act-implementation-timeline

[13] Federal "Temporary Pause" of State AI Laws Clears Procedural Hurdle as Sides Draw Battle Lines. (2025, June 18). Regulatory Oversight. https://www.regulatoryoversight.com/2025/06/federal-temporary-pause-of-state-ai-laws-clears-procedural-hurdle-as-sides-draw-battle-lines/

[14] From Graceland to Capitol Hill: The ELVIS Act's First Year Becomes a National Headliner. (2025, June 25). IP Law Group LLP. https://www.iplawgroup.com/from-graceland-to-capitol-hill-the-elvis-acts-first-year-becomes-a-national-headliner/

[15] Legal Risks for Small Businesses Using Artificial Intelligence Tools: What You Need to Know. (n.d.). Three Point Law. https://www.threepointlaw.com/the-recap/legal-risks-for-small-businesses-using-artificial-intelligence-tools-what-you-need-to-know

[16] Mitigating the Legal Risks of AI Systems. (n.d.). Heller Search Associates. https://www.hellersearch.com/blog/mitigating-the-legal-risks-of-ai-systems

[17] Navigating the California AI Transparency Act: New Contract Requirements. (2025, January 31). Orrick, Herrington & Sutcliffe LLP. https://www.orrick.com/en/Insights/2025/01/Navigating-the-California-AI-Transparency-Act-New-Contract-Requirements

[18] Navigating the EU AI Act: A Practical Guide to AI Compliance. (n.d.). MHP – A Porsche Company. https://www.mhp.com/en/insights/blog/post/eu-ai-act

[19] The One Big Beautiful Bill Act's Proposed Moratorium on State AI Legislation: What Healthcare Organizations Should Know. (2025, June 17). Sheppard Mullin Richter & Hampton LLP. https://www.sheppardhealthlaw.com/2025/06/articles/artificial-intelligence/the-one-big-beautiful-bill-acts-proposed-moratorium-on-state-ai-legislation-what-healthcare-organizations-should-know/

[20] The Senate's AI Ban Applies to Every State, Not Just BEAD Recipients. (n.d.). Center for American Progress. https://www.americanprogress.org/article/the-senates-ai-ban-applies-to-every-state-not-just-bead-recipients/

[21] Tennessee - Rothman's Roadmap to the Right of Publicity. (2025, March 3). Rothman's Roadmap to the Right of Publicity. https://rightofpublicityroadmap.com/state_page/tennessee/

[22] Texas Signs Responsible AI Governance Act Into Law. (2025, June 23). Latham & Watkins LLP. https://www.lw.com/en/insights/texas-signs-responsible-ai-governance-act-into-law

[23] Texas: Responsible Artificial Intelligence Governance Act - what businesses need to know. (2025, June 23). DataGuidance. https://www.dataguidance.com/opinion/texas-responsible-artificial-intelligence

[24] The Utah AI Act. (n.d.). Adeptiv. https://adeptiv.ai/utah-ai-act/

[25] US States Can (And Will) Continue To Regulate Artificial Intelligence … for Now. (n.d.). Taft Stettinius & Hollister LLP. https://www.taftlaw.com/news-events/law-bulletins/u-s-states-can-and-will-continue-to-regulate-artificial-intelligence-for-now/

[26] Utah and Colorado Have New Artificial Intelligence Laws. (2024, July 1). Willkie Farr & Gallagher LLP. https://www.willkie.com/publications/2024/07/utah-and-colorado-have-new-artificial-intelligence-laws

[27] What Legal Risks Should Businesses Consider When Using AI? (2025, January 16). Gerrish Legal. https://www.gerrishlegal.com/faqs/what-legal-risks-should-businesses-consider-when-using-ai

[28] 5 Legal Risks of Using AI in Business. (n.d.). Montanaro Law. https://montanarolaw.com/5-legal-risks-of-using-ai-in-business/

[29] AI Liability and Negligence Cases: Who's Responsible? (n.d.). Ethos Risk Services. https://ethosrisk.com/blog/ai-liability-and-negligence-cases-whos-responsible/

[30] AI Litigation Claims. (n.d.). Federal Lawyer. https://federal-lawyer.com/corporate-compliance/artificial-intelligence/litigation-claims/

[31] Utah scales back reach of generative AI consumer protection law. https://www.davispolk.com/insights/client-update/utah-scales-back-reach-generative-ai-consumer-protection-law