

Connecticut's AI legislation – Part 2: Frontier models and synthetic content transparency

August 27, 2026 | Client Update | 7-minute read

The Connecticut Artificial Intelligence Responsibility and Transparency Act positions the state, alongside California and New York, at the forefront of AI regulation. Phased effective dates begin October 1, 2026.

Introduction

In this update, our second of three on the 74-page [Connecticut Artificial Intelligence Responsibility and Transparency \(CART\) Act](#), we will examine the law's frontier models and synthetic content transparency provisions. Our [prior update](#) focused on the portions of the CART Act related to automated employment-related decision technology (AEDT) and companion chatbots. Our next and final update will discuss the CART Act's AI subscription requirements and social media rules.

Despite ongoing discussion at the federal level of preempting at least some state AI laws, states continue to adopt regulatory frameworks to address perceived risks in the AI space at a significant pace. The Connecticut legislature went from zero to 60 by stitching together in a single bill what likely would have been six distinct bills in most states. Indeed, when Connecticut Governor Ned Lamont signed the [Connecticut Artificial Intelligence Responsibility and Transparency \(CART\) Act](#) into law on May 27, 2026, it became the nation's most comprehensive state AI law to date. Notably, Colorado replaced the Colorado AI Act (CAIA), which was previously the most comprehensive state AI law, with the decidedly narrower regulatory framework in the Colorado Automated Decision-Making Technology Act (ADMTA) the same month (see DPW [update](#)).

The breadth of the CART Act stems from its coverage of multiple AI applications and use cases, including AEDT, AI companion chatbots, frontier AI models, synthetic content transparency, AI subscription products and social media. Connecticut is not the first state to regulate these areas; frontier models and companion chatbots, for instance, have been a significant driver of recent state legislation in California, New York and beyond (see DPW updates [here](#), [here](#) and [here](#)). Similarly, states such as California, Utah and Washington have already enacted laws requiring the application of embedded digital signatures to GenAI content. As a result, Connecticut was able to borrow extensively from existing state regulatory frameworks in developing its own comprehensive legislation.

Frontier models

Applicability

Starting October 1, 2026, the CART Act imposes requirements on “frontier developers” and “large frontier developers.” The Act defines “frontier developers” as entities that use a quantity of computing power greater than 10^{26} integer or floating-point operations and “large frontier developers” as frontier developers with annual gross revenues in excess of

\$500 million, consistent with California's [Transparency in Frontier AI Act \(TFAIA\)](#) and New York's [Responsible AI Safety and Education \(RAISE\) Act](#).

Requirements

Despite their similar definitions of frontier developers, the CART Act's scope is considerably narrower than that of TFAIA and RAISE. Both TFAIA and RAISE require large frontier developers to publish a periodically updated "frontier AI framework" detailing their technical and organizational protocols for "catastrophic risks" and regularly submit summaries of risk assessments to the relevant government bodies. Both acts also require frontier developers to publish a transparency report detailing the frontier model's intended uses, supported languages and output modalities, and any use restrictions, with an additional requirement for large frontier developers to disclose the results of catastrophic risk assessments before deploying new or substantially modified models.

By contrast, the CART Act imposes no public disclosure obligations on developers and focuses exclusively on whistleblower protections for their employees that largely mirror those of TFAIA.

First, all frontier developers are prohibited from retaliating against covered employees – those responsible for assessing and managing specified AI-related risks – for reporting activity that they reasonably believe presents a specific and substantial danger to public health and safety due to a "catastrophic risk." The CART Act defines "catastrophic risk" similarly to both the RAISE Act and TFAIA, as the risk that a frontier developer will materially contribute to the death of (or serious injury to) more than 50 people, or to the loss of more than \$1 billion in property. The developer's material contribution must occur in the form of a single incident in which the frontier model either:

- Provides expert-level assistance in the creation or release of a chemical, biological, radiological or nuclear weapon; or
- Engages in conduct with no meaningful human oversight, intervention or supervision that is either a cyberattack or, if the conduct had been committed by a human, would constitute the crime of murder, assault, extortion or theft, including theft by false pretenses.

Second, the CART Act also requires that, by January 1, 2027, each large frontier developer establish a reasonable internal process through which covered employees can anonymously report catastrophic risk concerns. Large frontier developers must also furnish reporting employees with updates regarding the investigation and actions taken in response. At least quarterly, each large frontier developer must provide its officers and directors with all catastrophic risk reports, and any officers or directors alleged in these reports to have engaged in wrongdoing may not receive or review them.

Third, all frontier developers must ensure their covered employees receive notice of these rights, through either postings in the workplace and equivalent distributions for new and remote employees or annual employee acknowledgements.

Enforcement

The CART Act empowers the Connecticut Attorney General to seek civil penalties of up to \$1,000 per violation, injunctive or equitable relief, as well as costs associated with bringing an action for each violation of the foregoing provisions. Significantly, neither injunctive nor equitable relief may be stayed pending appeal, which could compound the impact of any interim ruling. In contrast, TFAIA offers a private right of action.

Synthetic content transparency

Applicability

Article 50 of the [EU AI Act](#) imposed certain transparency requirements on both providers and deployers of AI systems to help ensure that consumers can distinguish AI-generated (or synthetic) content from human-generated (or authentic) content, effective August 2, 2026. Various states have enacted less stringent frameworks to foster transparency – for example, California's AI Transparency Act ([here](#), and [as amended](#)), Washington's [HB 1170](#) and Utah's [Digital Content Provenance Standards Act](#). As in other areas, the CART Act borrows extensively from these pre-existing frameworks.

All four statutes share a definition of provenance data: data that is embedded in digital content for the purpose of determining the content's authenticity, origin or modification history. All four statutes require providers whose GenAI systems have more than one million monthly users and are publicly accessible to consumers for personal use ("covered

providers”) to embed provenance data, though the CART Act excludes federal, state or local government agencies. The CART Act also excludes purely business-to-business uses, sales, licensing or distribution of GenAI systems, as well as video games and certain interactive experiences.

Additionally, while the CART Act and Washington’s HB 1170 limit their obligations to covered providers, the California AI Transparency Act and the Utah Digital Content Provenance Standards Act cast a wider net by imposing similar requirements on large online platforms, which must detect and label AI-generated content using provenance data, and manufacturers of “capture devices” like cameras, which must provide users with the option to include provenance data in content captured by the device.

Requirements

Starting October 1, 2026, the CART Act requires covered providers, to the degree commercially and technically reasonable, to include provenance data in any audio, image or video content created or materially altered by its GenAI system. Covered providers must also use commercially and technically reasonable methods to make provenance data difficult to tamper with or remove from their content, and to embed the provenance data in a manner that allows consumers to assess whether the content was created or altered by GenAI. The CART Act specifies that information about identified or reasonably identifiable individuals, trade secrets or proprietary GenAI design information need not be included in provenance data.

By comparison, the Utah Digital Content Provenance Standards Act takes a narrower approach, requiring only a latent disclosure that conveys the time and date of creation or alteration, along with either the name of the capture device manufacturer or digital signatures sufficient to prove AI involvement. The California AI Transparency Act, however, is the most expansive of the four, requiring covered providers to make available a free AI detection tool, while also imposing both a mandatory latent disclosure – including the provider’s name, system name and version number, time and date of creation or alteration, and a unique identifier – and the option for consumers to also include a manifest disclosure. Further, California requires that its disclosures be detectable by the aforementioned detection tool, consistent with “widely accepted” industry standards, and permanent or extraordinarily difficult to remove.

Enforcement

Like the AEDT and companion chatbot provisions, the Connecticut Attorney General has exclusive authority to enforce violations of the content provenance provisions as unfair or deceptive trade practices under the Connecticut Unfair Trade Practices Act. The CART Act provides no private right of action.

Key takeaways

- Companies that qualify as frontier developers under the CART Act should consider updates to employment policies and practices to integrate the Act’s whistleblower protection requirements.
- Companies that qualify as “covered providers” under the CART Act will need to evaluate and test approaches and technical methods of embedding relatively tamper-proof provenance data in GenAI content, and those operating in multiple states should consider undertaking a holistic legal review to ensure their chosen method is compliant across all relevant jurisdictions.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Matthew J. Bacal

+1 212 450 4790
matthew.bacal@davispolk.com

James W. Haldin

+1 212 450 4059
james.haldin@davispolk.com

David Lisson

+1 650 752 2013
david.lisson@davispolk.com

Howard Shelanski

+1 202 962 7060
howard.shelanski@davispolk.com

David I. Feinstein

+1 212 450 3293
david.feinstein@davispolk.com

This communication, which we believe may be of interest to our clients and friends of the firm, is for general information only. It is not a full analysis of the matters presented and should not be relied upon as legal advice. This may be considered attorney advertising in some jurisdictions. Please refer to the firm's privacy notice for further details.