

Insights

CONNECTICUT QUIETLY ADDS AI DISCLOSURE MANDATE TO CONSUMER PRIVACY LAW

Oct 07, 2025

While much of the national attention has focused on the wave of state-level AI legislation introduced in 2025, Connecticut has quietly enacted a significant AI-related amendment to its existing consumer privacy framework. On June 25, 2025, Governor Lamont signed [Public Act No. 25-113](#) into law, amending the Connecticut Data Privacy Act (“CTDPA”) to include a new, mandatory disclosure requirement for businesses that use personal data to train artificial intelligence (“AI”) systems, specifically large language models (“LLMs”).

This amendment has garnered relatively little attention compared to headline-grabbing AI bills in California, Colorado, and New York. Yet it is broadly applicable to a large swath of companies operating nationally and should not be ignored.

NEW DISCLOSURE REQUIREMENT FOR AI TRAINING

Effective July 1, 2026, controllers subject to the CTDPA^[1] must update their consumer-facing privacy notices to include a clear and conspicuous statement disclosing whether they collect, use, or sell personal data for the purpose of training LLMs. The disclosure must be “reasonably accessible, clear and meaningful,” and kept current.

This requirement applies regardless of whether the data is used internally or sold to third parties for model training and. Importantly, also applies to vendors acting on the controller’s behalf.

COMPLIANCE CONSIDERATIONS

To meet this obligation and more generally as key steps of the organization’s AI governance program, controllers should:

- **Audit data processing activities** to determine whether personal data is used in LLM training, *directly or via vendors*. Importantly, this disclosure is not limited to high-risk AI systems or automated decision-making contexts. It applies broadly to any use of personal data in training LLMs, regardless of the downstream application. And given that the law does not define

LLMs, organizations should take a conservative approach in determining what AI systems fall within this requirement.

- **Coordinate with legal and technical teams** to ensure disclosures are accurate and reflect actual practices.
- **Review and revise privacy notices** ahead of the July 1, 2026 deadline.

Connecticut's approach integrating AI-specific obligations into its broader consumer privacy framework may serve as a model for other jurisdictions. For businesses, this means that AI-related compliance must be addressed as part of a unified privacy governance strategy.

If you have questions about how this amendment may affect your organization, or how to align your AI practices with evolving state privacy laws, please contact a member of our Data Privacy & AI team.

[1] The CTDPA applies to entities that (1) control or process the personal data of at least 35,000 consumers, (2) control or process consumers' sensitive data (excluding personal data controlled or processed solely for completing a payment transaction), or (3) offer consumers' personal data for sale.

RELATED CAPABILITIES

- Data Privacy & Security
- Retail & Consumer Products

MEET THE TEAM



Goli Mahdavi

Co-Author, San Francisco

goli.mahdavi@bclplaw.com

[+1 415 675 3448](tel:+14156753448)



Amy de La Lama

Co-Author, Boulder

amy.delalama@bclplaw.com

[+1 303 417 8535](tel:+13034178535)

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.