BCLP. Client Intelligent

Insights

CONNECTICUT'S ONLINE SAFETY ACT: THE SWISS ARMY KNIFE OF AI REGULATION

May 28, 2026

On May 27th, Governor Lamont signed into law, Connecticut Public Act No. 26-15, known as the Online Safety Act. This new law establishes a comprehensive regulatory framework for artificial intelligence (AI) and online platforms, with primary provisions becoming effective October 1, 2026. Other specific sections have staggered start dates, including those for AI companions (January 1, 2027) and covered online platforms (January 1, 2028).

The Online Safety Act was several years in the making, with earlier attempts to pass a comprehensive AI law failing under threat of veto by Governor Lamont. However, growing concerns around children's online safety likely helped get the Act across the finish line.

As its broad title suggests, the Act addresses a wide range of potential risks arising in distinct contexts, including consumer-facing AI subscriptions, frontier model development, automated hiring tools, and AI companion applications. Not surprisingly, the Act also imposes a number of age-related obligations. Below are some of the key areas to know.

COMPLIANCE OBLIGATIONS

The Act imposes varied requirements depending on the type of technology or service provided:

- **Subscription-based AI Providers**: In an effort to promote transparency and consumer protection, the Act requires providers of subscription-based AI services (such as ChatGPT, Google Gemini, and similar consumer-facing AI tools) to provide consumers with written notice of key terms, including qualitative or quantitative limitations on the technology (e.g., usage caps, accuracy limitations, or restrictions on permissible use cases), and obtain the consumer's written acceptance of those terms before use.
- **Frontier Developer Whistleblowers**: Developers of high-compute "frontier models" (i.e., generally considered to be the most advanced or cutting-edge general purpose models) are prohibited from retaliating against employees who report "catastrophic risks" from such models to public health or safety. Large developers with over $500 million in annual revenue must establish anonymous internal reporting processes for such risks by January 1, 2027.

- **Automated Employment-Related Decision Technology (AEDT)**: Businesses using AI to make or materially influence hiring, promotion, discipline, or discharge decisions must provide a written pre-use notice of such technology to applicants and employees. This notice must disclose: (1) That AEDT has been deployed; (2) The purpose of the technology and the nature of the employment-related decision; (3) The trade name of the technology; (4) The categories of personal data being analyzed and how that data will be assessed to reach a decision; and (5) The sources of that personal data and contact information for the deployer.
- **AI Companions**: These systems must include protocols to detect risks of suicide or self-harm, refer users to mental health resources, and refrain from claiming to be human beings. Stricter regulations apply to interactions with minors, including prohibitions on romantic or manipulative interactions.
- **Covered Platforms (Social Media)**: Operators must use age verification or obtain verifiable parental consent before providing algorithmic feeds to minors. They must also display Surgeon General warnings regarding mental health risks and implement default settings for minors that limit usage to one hour per day.

PENALTIES AND ENFORCEMENT

Most violations of the Act, including those related to subscriptions, AI companions, AEDT, and online platforms, are deemed unfair or deceptive trade practices under the Connecticut Unfair Trade Practices Act and are enforced solely by the Attorney General. The Act generally does not create a private right of action. Frontier developers, however, face a distinct penalty structure, with civil penalties of up to $1,000 per violation, and the state may recover investigation costs and attorneys' fees if it prevails in an action. Additionally, for certain employment-related AI violations occurring before 2028, the Attorney General may issue a notice of violation and allow the entity 60 days to cure the issue before bringing an action.

For a comprehensive overview of AI-related regulatory developments, visit BCLP's AI Legislation Map.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Partner; Chair – Global Data Privacy and Security Practice; and Global Practice Group Leader – Technology, Commercial & Data, Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Goli Mahdavi

Global AI Lead, San Francisco

goli.mahdavi@bclplaw.com
+1 415 675 3448
