

Intellectual Property & Technology Law Journal

Edited by the Technology and Proprietary Rights Group of Weil, Gotshal & Manges LLP

VOLUME 38 • NUMBER 9 • OCTOBER 2026

South Carolina Enacts Age-Appropriate Design Code Act Amid Emerging Legal Challenges

By Andrew Serwin and Madison Bucci

South Carolina has passed its Age-Appropriate Design Code Act (Act),¹ joining a growing number of states adopting “age-appropriate design code” (AADC)-style legislation that intends to reshape how online services design, operate, and monetize products likely to be accessed by minors.

Backed by robust enforcement mechanisms, the Act represents one of the most prescriptive children’s online safety laws to date. As a result, the law has already become the subject of constitutional litigation, underscoring the legal uncertainty surrounding design-based regulatory approaches.

This article summarizes the Act’s core requirements, highlights key differences from earlier AADC models, and discusses the initial legal challenge filed by NetChoice.

OVERVIEW OF THE ACT

The Act applies to “covered online services” – websites, applications, or online services that are reasonably likely to be accessed by minors and that meet certain revenue or data-processing thresholds. Like other AADC laws, South Carolina’s statute is

grounded in a “protection by design” framework, imposing affirmative obligations on covered services to proactively mitigate risks to minors arising from both data practices and product design.

Unlike earlier AADC statutes, South Carolina’s law enumerates specific design features, mandates default safeguards, and authorizes significant remedies for non-compliance.

KEY SUBSTANTIVE REQUIREMENTS

Duty of Reasonable Care to Prevent Harm

Central to the Act is an obligation for covered online services to exercise reasonable care in both their data practices and service design to prevent enumerated harm to minors, including:

- Compulsive usage;
- Severe psychological or emotional harm (including anxiety, depression, self-harm, or suicidal ideation);
- Highly offensive intrusions into reasonable privacy expectations; and
- Identity theft, discrimination, and material financial or physical injury.

The authors, attorneys with DLA Piper, may be contacted at andrew.serwin@us.dlapiper.com and madison.bucci@us.dlapiper.com, respectively.

This “reasonable care” obligation reflects a departure from traditional notice-and-consent privacy frameworks in favor of substantive design-based accountability for online services.

Notably, the statute limits the definition of “harm” to a harm for which liability is permitted under 47 U.S.C. § 230, including as that provision may be amended or repealed in the future. This built-in limitation may shape both the scope of the duty and available defenses in enforcement actions.

Explicit Regulation of “Covered Design Features”

South Carolina’s Act is more detailed than earlier AADC laws in its definition and regulation of “covered design features,” which are features that encourage or increase a minor’s frequency, time spent, or activity on an online service. The statute expressly identifies certain features such as:

- Infinite scroll;
- Auto-playing videos;
- Gamification (e.g., streaks, badges, and rewards);
- Quantification of engagement (e.g., likes, views, comments, and reactions);
- Notifications and push alerts;
- In-game purchases; and
- Appearance-altering filters.

Covered services must configure default settings for minors who disable non-essential engagement-driving features and provide tools to manage or disable such features. This level of specificity distinguishes South Carolina’s approach from jurisdictions that rely on broader concepts, such as “addictive feeds,” and significantly constrains product and interface design choices for services within scope.

Default Safeguards and User Controls

For users who are known to be minors, covered services must implement default settings that include the ability to:

- Opt out of personalized recommendation systems;
- Limit time spent on the service;
- Disable engagement metrics (e.g., likes and views);
- Restrict messaging from non-connected accounts;
- Prevent search engine indexing of profiles; and
- Restrict visibility of location information.

All such safeguards must be set at the highest level of protection by default, reinforcing the Act’s emphasis on default design rather than user choice.

Data Minimization and Advertising Restrictions

The Act imposes strict data protection obligations, including:

- Limits on the collection, use, and sharing of personal data to what is strictly necessary;
- Prohibition on the use of minors’ data for secondary purposes;
- Mandatory deletion of age-verification data after use;
- A categorical ban on targeted advertising to minors;
- A separate prohibition on advertisements for products that are prohibited for minors, including narcotic drugs, tobacco products, gambling, and alcohol, distinct from the general targeted advertising restriction; and
- Restrictions on the default collection of precise geolocation data.

These requirements align with broader trends in state children’s privacy laws but are notable for their breadth and lack of safe harbors tied to consent.

Notification Curfews and School-Hour Restrictions

The Act includes some of the most detailed notification restrictions enacted to date. Covered services must offer tools to prevent notifications to minors:

- Between 10:00 p.m. and 6:00 a.m., year round; and
- Between 8:00 a.m. and 3:00 p.m., Monday through Friday, during the school year (August to May).

These provisions directly regulate product functionality based on time of day, raising operational and technical compliance considerations.

Parental Tools and Transparency

Covered services must provide parental monitoring and control tools, enabled by default, including the ability to manage privacy settings, restrict purchases, and view total time spent on the service. Importantly, the Act requires clear notice to minors when parental monitoring is active.

In addition, covered services must publish annual public reports, prepared by independent third-party auditors, detailing their design features, data practices, algorithms, and risk-mitigation measures relating to minors. These reports must be submitted to, and publicly posted by, the South Carolina Attorney General.

Enforcement and Remedies

The Act is enforced by the South Carolina Attorney General and authorizes:

- Personal liability for officers and employees in cases of willful and wanton misconduct;
- Treble damages for violations; and
- Treatment of dark patterns as unlawful trade practices under South Carolina law.

IMMEDIATE LEGAL CHALLENGE BY NETCHOICE

As anticipated, NetChoice has filed a lawsuit challenging the Act, seeking declaratory and injunctive relief on constitutional grounds.

NetChoice argues, among other things, that:

- The Act's "reasonable care" requirement functions as a content-based restriction on speech, rendering it subject to, and unable to survive, strict scrutiny under the First Amendment;
- The law is overinclusive and underinclusive, regulating vast categories of protected expression while failing to directly address certain harms;
- The Act is pre-empted by Section 230 of the Communications Decency Act and the Children's Online Privacy Protection Act (COPPA); and
- Key provisions are unconstitutionally vague, particularly with respect to design-based obligations and harm prevention.

In a notable early development, Governor Henry McMaster moved to intervene as a defendant. While the precise rationale for the governor's intervention remains unclear, the move could signal the state's interest in defending the Act and ensuring a robust presentation of its constitutional arguments.

PRACTICAL TAKEAWAYS

- Compliance planning is encouraged to continue. Despite the pending litigation, covered services may assess whether their products fall within scope and identify design features regulated by the Act.
- Design and product teams face heightened risk. South Carolina's law goes beyond data governance, directly regulating interface and engagement mechanics.
- Litigation risk could remain high. As with similar laws in California and elsewhere, enforcement timelines and ultimate viability may depend on the outcome of constitutional challenges.

Note

1. https://www.scstatehouse.gov/sess126_2025-2026/prever/3431_20260114.htm.

Copyright © 2026 CCH Incorporated. All Rights Reserved.
Reprinted from *Intellectual Property & Technology Law Journal*, October 2026, Volume 38,
Number 9, pages 25–27, with permission from Wolters Kluwer, New York, NY,
1-800-638-8437, www.WoltersKluwerLR.com



Wolters Kluwer