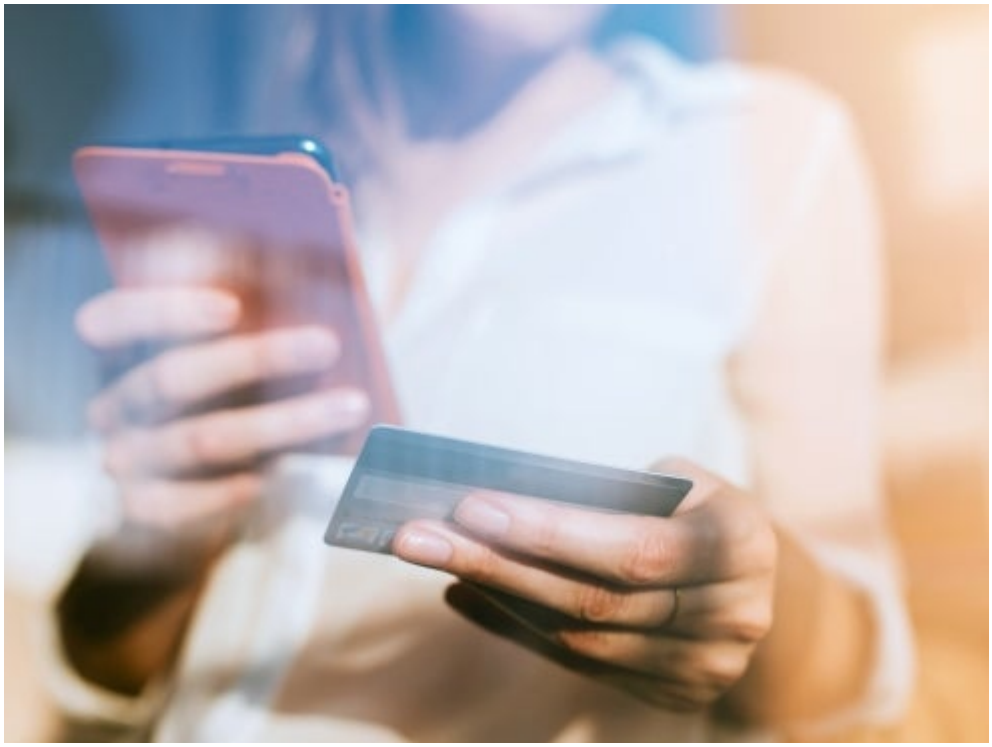
Blogs
October 09, 2023
Federal Courts Preliminarily Enjoin Arkansas Social Media Safety Act and California Age-Appropriate Design Code



After a flurry of legislative activity across the United States related to kids' privacy and safety online, in recent weeks, federal courts in Arkansas and California have enjoined two notable state laws.

A federal court in Arkansas preliminarily enjoined the Arkansas Social Media Safety Act (AR SMSA) on August 31, the day before the statute was scheduled to take effect for social media platforms in scope. The U.S. District Court for the Western District of Arkansas found that the plaintiff, NetChoice, LLC, is likely to succeed on the merits of its constitutional challenges.

Less than three weeks later, on September 18, the U.S. District Court for the Northern District of California also preliminarily enjoined California's Age-Appropriate Design Code (CA AADC), holding that NetChoice is likely to succeed in showing that 10 CA AADC requirements violate the First Amendment.

This post provides a brief overview of each decision and what may happen next.

AR SMSA Scoping Standard

As described here, the Arkansas law would impose age verification and parental consent requirements on social media platforms that allow individuals to create an account or public profile for the "primary purpose" of interacting socially with other users. Covered social media platforms would be required to verify the age of all account holders who reside in Arkansas and obtain parental consent for all Arkansas minors under 18 prior to account creation.

In granting the preliminary injunction in Arkansas, the court found that the Arkansas law's scoping standard for "social media platforms" was unconstitutionally vague because it failed to adequately define which companies

are subject to its verification and parental control requirements. The court noted that the statute neither defines "primary purpose" nor provides guidelines on how to determine a platform's purpose. Similarly, the court determined that the law fails to adequately define the proof necessary to establish that a platform has obtained "express consent" from a parent or guardian.

AR SMSA First Amendment

In regard to NetChoice's First Amendment challenge, the court held that the law's age verification and parental consent requirements are not narrowly tailored to the state's interest in protecting children online. As a result, the court determined that the age verification requirement unconstitutionally burdens adult and minor access to protected speech. Rather than requiring specific content filters or limitations—which the court suggests may be constitutional under U.S. Supreme Court doctrine—the Arkansas statute unconstitutionally impedes access to all content on covered platforms.

CA AADC First Amendment

Although the NetChoice complaint contained a number of claims—including that the law violated the dormant Commerce Clause of the U.S. Constitution and was preempted by the Children's Online Privacy Protection Act (COPPA)—the court focused its analysis on NetChoice's First Amendment claims, holding that NetChoice is likely to succeed in showing that the CA AADC's challenged mandates and prohibitions fail commercial speech scrutiny and are therefore invalid. *See NetChoice v. Bonta*, at 34. In so holding, the court reviewed 10 distinct CA AADC requirements. The below excerpts provide a snapshot of the court's reasoning for several of the requirements:

- **Data protection impact assessments (DPIAs).**[1]**"**Because the DPIA report provisions do not require businesses to assess the potential harm of the design of digital products, services, and features, and also do not require actual mitigation of any identified risks, the State has not shown that these provisions will 'in fact alleviate [the identified harms] to a material degree.'" *Id. at* 21.
- **Estimate the age of users or apply children's privacy settings to all consumers. "**[I]f a business chooses not to estimate age but instead to apply broad privacy and data protections to all consumers, it appears that the inevitable effect will be to impermissibly 'reduce the adult population to reading only what is fit for children.'" *Id.* at 24. Additionally, "such an effect would likely be, at the very least, a 'substantially excessive' means of achieving greater data and privacy protections for children." *Id*.
- **Age-appropriate policy language.** Responding to the state's argument that the provision "'protects the safety and well-being of minors' by 'giving children the tools to make informed decisions about the services with which they interact,'" the court noted that the state had shown that "internet users generally do not read privacy policies, and that the reason may be that such policies are often 'written at the college level and therefore may not be understood by a significant proportion of the population (much less children).'" *Id.* at 25-26. The court continued, "[e]ven accepting that the manner in which websites present 'privacy information, terms of service, policies, and community standards,' constitutes a real harm to children's well-being because it deters children from implementing higher privacy settings, the State has not shown that the CA AADC policy language provision would directly advance a solution to that harm." *Id.* at 26 (citation omitted).
- **Requirement to enforce published terms, policies, and community standards established by the business.** The state did not establish a "causal link between whether a business consistently follows its 'published terms, policies, and community standards'—or even children's difficulty in making better-informed decisions about whether to use online services—and some harm to children's well-being." *Id.* at 27. Moreover, the "required commitment [to follow policies the business wishes to set]…flies in the face of a platform's First Amendment right to choose in any given instance to permit one post but prohibit a

substantially similar one." *See id.*

- **Restriction on using a child's personal information for any reason other than a reason for which that personal information was collected.** "[T]he State provides no evidence of a harm to children's well-being from the use of personal information for multiple purposes." *Id.*
- **Restriction on use of dark patterns.** "[T]he State has not shown that dark patterns causing children to forego privacy protections constitutes a real harm." *Id.* at 33.

AR SMSA and CA AADC Next Steps

While both states are expected to appeal, in the meantime, the preliminary injunctions may lead to challenges against statutes with similar characteristics in other states. State legislatures may also choose to amend adopted laws or pending bills in anticipation of similar challenges.

Other Children's Privacy and Safety Regulations

Despite the preliminary injunctions in Arkansas and California, there remains a clear trend in the United States and Europe to further regulate children's privacy and safety online. In the United States, seven other states have recently passed children's privacy and/or safety laws, with a number of bills in other states still pending. In Europe, the UK Age-Appropriate Design Code, Ireland's Fundamentals for a Child-Oriented Approach to Data Processing, and the Netherlands Code for Children's Rights are all examples of age-appropriate design codes that address similar issues.

In addition to existing age-appropriate design codes, the UK Parliament recently passed its Online Safety Bill which will (upon royal assent) impose risk assessment, content moderation, and age assurance requirements on a variety of online services that enable user-generated content.

Finally, the European Commission's Special Group on a Code of Conduct for Age-Appropriate Design convened for the first time on July 12, 2023. The group is tasked with drafting a comprehensive code of conduct for age-appropriate design that will encourage responsible behavior for parties involved with children in the digital sphere.

Companies that are potentially in scope for children's privacy and safety regulations may wish to identify any compliance needs arising from this fast-changing area of the law.

---

[1] The DPIA requirement would require in scope businesses to review an online product, service, or feature for certain risks, including "whether the design of the online product, service, or feature could harm children, including by exposing children to harmful, or potentially harmful, content…[.]" Cal. Civ. Code Sec. 1798.99.31(a)(1)(B)(i).

Authors

Explore more in

Privacy & Security