

April 3 Update: Injunction on California AADC Partially Vacated—Key Provisions Now in Effect

March 24, 2026

APRIL 3 STATUS UPDATE: The Ninth Circuit issued its mandate on April 3, 2026—meaning that many previously-enjoined provisions (outlined in more detail below) of the California Age-Appropriate Design Code Act (AADC) are now in effect.

On March 12, 2026, the U.S. Court of Appeals for the Ninth Circuit released an opinion that partially vacates a lower court’s injunction of the California Age-Appropriate Design Code Act (AADC), allowing elements of the AADC to take effect as soon as April 2, absent further judicial action.

The AADC imposes strict requirements on businesses that provide an online service, product, or feature that is “likely to be accessed by children.” Importantly, the AADC defines a “child” as an individual under the age of 18.

The key provisions of the AADC that may now take effect include requirements related to estimating minors’ ages, implementing high-privacy default settings, providing age-appropriate notices, providing monitoring or tracking signals, and providing privacy rights tools. The court affirmed the injunctions regarding certain uses of a minor’s data and so-called “dark patterns.”

NetChoice v. Bonta: The Latest Chapter in the AADC Saga

The Ninth Circuit’s March 12, 2026, *NetChoice v. Bonta* decision is the latest chapter in a legal challenge that began after California enacted the AADC in 2022.[1] As we previously explained, the AADC goes well beyond the requirements of the federal Children’s Online Privacy Protection Act (COPPA) in both its scope and its substantive

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Boyd Garriott
Associate
202.719.4487
bgarriott@wiley.law

Stephanie Rigizadeh
Associate
202.719.4736
srigizadeh@wiley.law

Practice Areas

Advertising Technology (AdTech) Data
Privacy and Consumer Protection
Cyber and Privacy Investigations, Incidents
& Enforcement
FTC and Consumer Protection
Privacy, Cyber & Data Governance
State Privacy Laws

reach, particularly as it defines a child as being under the age of 18 (a minor).

In 2024, the Ninth Circuit affirmed a preliminary injunction against two AADC provisions: (1) the requirement to prepare Data Protection Impact Assessments (DPIAs) and (2) a notice-and-cure provision referencing the DPIA requirement.

In the recent 2026 decision, the Ninth Circuit determined that the DPIA requirement “remains enjoined and is not at issue in this appeal.”[2] Additionally, the Ninth Circuit upheld a district court injunction against two additional AADC elements: (i) certain restrictions on the use of children and teen data and (ii) restrictions on the use of “dark patterns,”[3] discussed further below.

The Ninth Circuit’s decision allowed the remaining elements of the law to take effect.

Which Parts of the California AADC Remain Standing?

Absent further appellate action, the remaining AADC obligations will spring into effect when the Ninth Circuit issues its mandate. The mandate is expected on April 2 at the earliest, or 7 days after the March 26 rehearing deadline under the Federal Rules of Appellate Procedure.

Under these provisions, businesses providing “an online service, product, or feature likely to be accessed by children” must:

- **Estimate Minors’ Age:** Covered businesses must “[e]stimate the age of child users with a reasonable level of certainty appropriate to the risks that arise from the data management practices of the business or apply the privacy and data protections afforded to children to all consumers.”
- **Implement High-Privacy Default Settings:** Covered businesses should “[c]onfigure all default privacy settings provided to children by the online service, product, or feature to settings that offer a high level of privacy, unless the business can demonstrate a compelling reason that a different setting is in the best interests of children.”
- **Provide Age-Appropriate Notices:** Covered businesses should “[p]rovide any privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age of children likely to access that online service, product, or feature.”
- **Monitoring or Tracking Signals:** “If the online service, product, or feature allows the child’s parent, guardian, or any other consumer to monitor the child’s online activity or track the child’s location, provide an obvious signal to the child when the child is being monitored or tracked.”
- **Privacy Policy Enforcement:** Covered businesses must “[e]nforce published terms, policies, and community standards established by the business, including, but not limited to, privacy policies and those concerning children.”
- **Privacy Rights Tools:** Covered businesses should “[p]rovide prominent, accessible, and responsive tools to help children, or if applicable their parents or guardians, exercise their privacy rights and report concerns.”

Additionally, covered businesses are prohibited from:

- **Collecting, Selling, or Sharing Minors' Precise Geolocation Information:** Covered businesses may only engage in the practice if collection "is strictly necessary for the business to provide the service, product, or feature requested." In such a case, collection must occur "for the limited time . . . necessary to provide the service, product, or feature."
- **Collecting Precise Geolocation Without "An Obvious Sign" to the Minor:** This sign should last "for the duration of that collection that precise geolocation information is being collected."
- **Using Personal Information to Estimate Age "For Any Other Purpose" or Retain the Information "Longer Than Necessary to Estimate Age:"** Under the AADC, "[a]ge assurance shall be proportionate to the risks and data practice of an online service, product, or feature."

Which Provisions of the Injunction Did the Ninth Circuit Keep?

- Restrictions on Data Use, including:
 - Limitations on the use of a minor's personal information, particularly if "the business knows, or has reason to know" that the information "is materially detrimental to the physical health, mental health, or well-being of a child."
 - Prohibition on profiling a minor without "appropriate safeguards," and the profiling must be "necessary to provide the online service, product, or feature" or "in the best interests of the" minor.
 - Prohibition on collecting, selling, sharing, or retaining "any personal information that is not necessary to provide an online service, product, or feature . . . unless the business can demonstrate a compelling reason that the collecting, selling, sharing, or retaining of the personal information is in the best interests of children likely to access the online service, product, or feature." Prohibition on the use of minors' personal information for reasons other than that for which the business collected the information, absent showing that the use is "in the best interests" of the minors.
- Restrictions on "Dark Patterns": Businesses cannot use "dark patterns to lead or encourage children to provide personal information beyond what is reasonably expected to provide that online service, product, or feature to forego privacy protections, or to take any action that the business knows, or has reason to know, is materially detrimental to the child's physical health, mental health, or well-being."

Which Businesses Are Covered by the AADC?

The AADC covers any "business that provides an online service, product, or feature likely to be accessed by children." The AADC uses the definition of "Business" under the California Consumer Protection Act (CCPA). Under the CCPA, a "business" includes any "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity . . . that collects consumers' personal information, or on the behalf of which such information is collected and . . . determines the purposes and means of the processing of consumers' personal information, that does business in the State of California." The business must also meet at least **one** of the following thresholds:

- Has gross revenue exceeding \$25,000,000 (adjusted to reflect increases in the Consumer Price Index), as of January 1 of the calendar year;
- Buys, sells, or shares personal information of 100,000 or more consumers or households; or
- Obtains more than 50% of revenue from selling or sharing customers' personal information.

An "online service, product, or feature" does not include broadband internet access service as defined under the California code, a telecommunications service, or the delivery or use of a physical product.

Under the AADC, "likely to be accessed by children" means that the businesses' online service, product, or feature is:

- Directed to children, as defined under COPPA;
- Determined, "based on competent and reliable evidence regarding audience composition, to be routinely accessed by a significant number of children;"
- Marketed to minors;
- Substantially similar or the same as an online service, product, or feature routinely accessed by minors;
- Includes design elements of interest to children, such as games, cartoons, music, and celebrities; or
- Generates a significant audience of minors, according to internal research.

Moving forward, companies should reassess whether their services and products fall into these categories, particularly given the applicability of this law to minors under the age of 18.

Looking Ahead

The Ninth Circuit's decision adds an additional layer of complexity to businesses' compliance with the AADC. Future proceedings, including rehearing at the Ninth Circuit or the Supreme Court's grant of certiorari, if filed, would change the AADC compliance landscape. As the future of the AADC unfolds, businesses should examine compliance with the current obligations.

Wiley's Privacy, Cyber & Data Governance practice has a deep bench of attorneys guiding companies through a broad range of risk management and policy compliance under state and federal privacy frameworks. If you have questions or would like more information about your company's privacy compliance, please contact one of the authors of this alert.

[1] *NetChoice v. Bonta*, No. 25-2366 (9th Cir. 2026).

[2] *Id.* at 8.

[3] *Id.* at 34-41.