**No. 23-2969**

**IN THE UNITED STATES COURT OF APPEALS**
**FOR THE NINTH CIRCUIT**

---

*NetChoice, LLC,*
*Plaintiff-Appellee*

*v.*

*Rob Bonta,*
*Attorney General of the State of California,*
*in his official capacity,*
*Defendant-Appellant.*

---

On Appeal from the United States District Court for the
Northern District of California
No. 5:22-cv-08861
The Honorable Beth Labson Freeman, District Court Judge

---

# BRIEF OF THE ELECTRONIC PRIVACY INFORMATION CENTER AS *AMICUS CURIAE* IN SUPPORT OF DEFENDANT-APPELLANT SUPPORTING REVERSAL

---

Megan Iorio
Tom McBrien
Suzanne Bernstein
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140
iorio@epic.org

December 20, 2023

*Attorneys for Amicus Curiae*

## CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1, *amicus curiae* the Electronic Privacy Information Center states that it has no parent corporation and that no publicly held corporation owns 10% or more of its stock.

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

### Cases



### Statutes

**Other Authorities**

## INTEREST OF THE *AMICUS CURIAE*

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues.[1] EPIC advocates for meaningful government oversight of abusive, exploitative, invasive, and discriminatory data collection systems, algorithms, and platform design decisions. EPIC is interested in this case because of the organization's concern that the district court's overly broad First Amendment analysis, if adopted widely, would render nearly all regulations of internet companies unconstitutional and unenforceable.

EPIC regularly participates as *amicus* in this Court and other courts in cases concerning privacy rights, harmful data practices, the First Amendment, and platform accountability. *See, e.g.*, Br. of EPIC as Amicus Curiae, *NetChoice v. Paxton* (No. 22-555) (U.S.) (filed Dec. 7,

---

[1] All parties consent to the filing of this brief. In accordance with Rule 29, the undersigned states that no party or party's counsel authored this brief in whole or in part nor contributed money intended to fund the preparation of this brief. No outside person contributed money intended to fund the preparation of this brief.

2023); Br. of EPIC as Amicus Curiae, *Gonzalez v. Google*, 598 U.S. 617 (May 18, 2023); Br. of Epic as Amicus Curiae, *Wilkinson v. Facebook* (No. 22-16888) (9th Cir.) (filed Nov. 3, 2023); Br. of Epic et al. as Amici Curiae, *Bride v. Yolo Technologies, Inc.* (No. 23-55134) (9th Cir.) (filed Aug. 25, 2023); Br. of Epic et al. as Amici Curiae, *NetChoice, LLC v. Bonta*, No. 22-cv-8861-BLF, 2023 WL 6135551 (N.D. Cal. Sept. 18, 2023).

## SUMMARY OF THE ARGUMENT

One of the first major privacy laws passed in the United States in the modern internet era established special protections for children under 13 years of age and imposed strict requirements on operators of websites directed to those young audiences. Since the Children's Online Privacy Protection Act was passed in 1998, lawmakers at the federal and state level have introduced and passed a wide range of statutes aimed at securing privacy and at protecting kids online. The rule adopted by the lower court would call all these laws into question by imposing heightened First Amendment scrutiny and questioning the means-ends fit of privacy laws that also require some estimation of user age. The lower court's decision is deeply flawed because it fails to recognize the state's substantial interest in protecting the privacy of children online and incorrectly analyzes the requirements of the California Age-Appropriate Design Code ("AADC"). The lower court's analysis hinges in part on false assumptions that the AADC requires companies to limit access to content and to deploy invasive age verification techniques. The AADC does not require either of those things, and its privacy and design-focused requirements allow for a

flexible approach to age estimation that incentivizes companies to provide heightened privacy protections to all users to mitigate harms to children. The AADC is fundamentally different from other statutes that seek to prohibit children's access to online content or services and, thereby, impose substantial age verification burdens on adult users.

## ARGUMENT

### I. THE AADC PROMOTES KIDS' SAFETY ONLINE BY PROTECTING THEM FROM ABUSIVE DATA PRACTICES, NOT BY LIMITING THEIR ACCESS TO ONLINE SERVICES.

The AADC is a privacy law that regulates how internet companies collect, manage, and use children's personal information. The law does not prohibit companies from showing any type of content, nor does it segregate the internet into adult-only and child-only zones. Instead, it simply tasks companies with adopting a baseline of privacy protection for children and with adhering to basic reporting requirements that incentivize companies to consider how their data management practices affect children.

The AADC has three main components: a data protection impact assessment ("DPIA") requirement, privacy and data protection

mandates, and the option to either provide the privacy and data protections to all users or to provide them only to users they believe are likely to be children. The DPIA provision requires companies to assess how their services use kids' personal data and to what extent these data practices create risks for children. The privacy and data protection mandates require companies to limit the collection, use, storage, and disclosure of kids' (or all users') personal information. Companies that choose to apply these protections to only child users must estimate the age of users to a level of certainty proportional to the risk of harm determined by the DPIA. The greater the risk posed by a company's data practices, the higher the level of certainty that that company should have in estimating user age in order to properly implement the privacy protections required for child users.

The district court below failed to appreciate the specific privacy harms that the commercial collection and use of personal information poses to children and failed to recognize that the AADC is designed to address these harms. The AADC's assessment and privacy protection mandates are all tied to the *use of kids' personal information* and do not direct companies to block any content or exclude any users.

### A. The data protection impact assessment provision requires companies assess how their collection and use of kids' user data might create several enumerated risks of harm to kids.

The core component of the AADC is a requirement that companies closely review their products and services with a focus on how they collect and use kids' data and the potential harmful impacts that those data uses have. Policymakers have long recognized the harmful impact that commercial surveillance, targeted advertising, and profiling can have on children. A requirement that companies closely consider these impacts and modify their practices to avoid predictable harms is the bare minimum that the law should require.

As the name suggests, data protection impact assessments, or DPIAs, are used to identify the risks companies' *data* practices create for user privacy. The AADC's DPIA requirement is no different. The statutory definition of the DPIA is "a systematic survey to assess and mitigate risks that arise from the ***data management practices*** of the business to children who are reasonably likely to access the online service, product, or feature at issue that arises from the provision of

that online service, product, or feature." Cal. Civ. Code § 1798.99.30(b)(2) (emphasis added).

The areas of assessment that a DPIA must cover are also explicitly limited to a company's *data* practices. Under the AADC, companies must identify three things in their DPIA for each online service, product, or feature likely to be accessed by a child: (1) "the purpose of the online service, product, or feature," (2) "how [the service, product, or feature] ***uses children's personal information***," and (3) "the risks of material detriment to children that arise ***from the data management practices*** of the business." *Id.* § 1798.99.31(a)(1)(B) (emphasis added). The law then enumerates several risks of harm that companies must assess their data practices for. *Id.* §§ 1798.99.31(a)(1)(B)(i)–(viii).

Each of these risks is to be assessed based on whether the companies' *data* practices are likely to cause the specified harm. For instance, companies must look at the likelihood that *their use of kids' personal information* will lead to them being "targeted by harmful, or potentially harmful, contacts," *id.* § 1798.99.31(a)(1)(B)(ii), and whether

their *use of kids' personal information* in their targeted advertising system could harm children, *id.* § 1798.99.31(a)(1)(B)(vi).

The requirement that companies assess "whether the design of the online product, service, or feature could harm children, including by exposing children to harmful, or potentially harmful, content on the online product, service, or feature," *id.* § 1798.99.31(a)(1)(B)(i), has been misinterpreted as a requirement that companies assess whether kids can access harmful content on their services. This provision is much more narrowly focused on how a company's *use of kids' personal information* creates a risk that their service *directs* kids to harmful, or potentially harmful, content, not whether they host the content or make it available at all.

The use of personal information to target specific content to kids poses unique risks, many of which companies are already well aware. Many internet companies today employ recommendation algorithms that target advertisements or recommend content to users based on extensive behavioral profiles. Arvind Narayanan, Knight First Amendment Institute, *Understanding Social Media Recommendation*

*Algorithms* 24 (Mar. 9, 2023).[2] Because time spent on the platform translates into revenue from ads, companies collect vast amounts of personal data on users to predict what presentation of content will keep users on the platform longest. *Id.* at 35. The behavioral profiles contain thousands of data points and are so powerful that they can be used to infer personal information that wasn't explicitly collected, such as a user's age, gender, race, and interests. *Id.* at 22. The drive to design algorithms that better predict user behavior leads companies to collect more and more personal information, fueling an ever more invasive commercial surveillance system.

Companies design their recommendation algorithms to maximize the probability that a user will interact with the posts they are shown—a concept the industry calls "engagement." *Id.* at 20. The myopic focus on maximizing engagement can lead companies to ignore the negative side-effects, such as targeting users with content that frightens, angers,

---

[2] https://knightcolumbia.org/content/understanding-social-media-recommendation-algorithms.

or induces anxiety in them because their behavioral profiles indicate they will engage more with that content.

Companies are not blind to the harms of engagement maximization. In a leaked document from Meta describing a study conducted about mental health among teens on Instagram, one slide explained that teens who were unsatisfied with their lives were more likely to be shown content that depicted negative messages, like not being attractive, not having friends, not being good enough, and even wanting to hurt or kill themselves. *Teen Mental Health Deep Dive,* Wall St. J. (Sep. 29, 2021).[3] Serving negative, harmful, or disturbing content has been shown to keep users on a platform longer. *See* Steve Rathje, Jay J. Van Bavel & Sander van der Linden, *Out-Group Animosity Drives Engagement on Social Media*, 118 Proceedings of the Nat. Acad. Sci. 1, 1 (2021). This content is tailored to the individual user, such as recommending content related to eating disorders to users who worry about their body image, and then showing them *more* of this content to

---

[3] https://s.wsj.net/public/resources/documents/teen-mental-health-deep-dive.pdf.

keep them on the platform. *See* Jennifer Neda John, *Instagram Triggered My Eating Disorder*, Slate (Oct. 14, 2021).[4] As one Meta employee said, the recommendation algorithm tends to pull young users into "negative spirals & feedback loops that are hard to exit from." Compl. ¶ 160, *California et al. v. Meta Platforms, Inc. et al.*, No. 4:23-cv-05448-YGR (Nov. 11, 2023). And while Meta tested tweaks to the design of its recommendation algorithm to reduce the probability that targeted recommendations based on behavioral profiles would create harmful content loops for kids, Meta decided against implementation because "it came with a clear engagement cost." *Id.* ¶ 221.

The AADC's DPIA provision thus requires companies to evaluate during the design process the potentially harmful impacts that use of kids' personal information may have. Most companies do not sufficiently weigh these impacts currently or subserviate them to the quest for engagement.

---

[4] https://slate.com/technology/2021/10/instagram-social-media-eating-disorder-trigger.html.

It is worth noting that companies have a lot of discretion in making these assessments, which gives them more control over privacy obligations than they have under more restrictive statutes. The term "harm" only appears in the AADC in the DPIA section; companies are only required to modify their data practices to the extent *they* find that the practices would cause harm. *See* Cal. Civ. Code §§ 1798.99.31(a)(1)(B)(i)–(vii). Companies can also only be held liable for data uses that the company has assessed—or should have identified—as creating a risk of "material detriment to children." *See id.* §§ 1798.99.31(a)(1)(A)–(B). Companies only have an obligation to refrain from data use and dark patterns that "the business knows, or has reason to know, is materially detrimental to the physical health, mental health, or well-being of a child," *id.* §§ 1798.99.31(b)(1), (7)—that is, they are only prohibited from using kids' personal data or dark patterns in connection with the specific "material detriment[s]" the business has identified or should have identified. This regulatory scheme is a far cry from a top-down prohibition on any content that the government itself labels as harmful. *See infra* Section III (comparing the AADC's requirement to assess how use of kids' data can expose kids to harmful

content to other state laws that require companies to block specific categories of content.)

### B. The AADC limits harmful collection, use, and disclosure of personal information, which is common in privacy and data protection statutes.

Unlike laws that seek to exclude kids from certain online spaces, the AADC directs companies to give kids stronger privacy protections so that they can be *included* more safely. The AADC's privacy protections are meant to mitigate harms caused by online companies' extensive collection and use of kids' data, such as by reducing the structural incentives to optimize for engagement based on kids' behavior. Privacy requirements may change the way companies target information to users, but that is not the same as limiting user access to content.

First, the AADC limits how much data companies can collect, sell, share, and retain about children. The law includes a general data minimization requirement, meaning that companies must limit the personal information they collect, sell, share, and retain to what is necessary to provide a service with which a child is actively engaged. Cal. Civ. Code § 1798.99.31(b)(3). The law also limits the collection of precise geolocation information to what is "strictly necessary" to provide

the service. *Id.* § 1798.99.31(b)(5). Data minimization is a central aspect of emerging privacy frameworks, such as the American Data Privacy and Protection Act ("ADPPA"), which typically limit collection of sensitive categories of personal information like precise location data to situations where such collection is "strictly necessary" and limits all other collection of personal information to what is "necessary." *See* Caitriona Fitzgerald, EPIC, *A Proposed Compromise: The State Data Privacy and Protection Act* (Feb. 22, 2023).[5] The AADC arguably offers more flexibility to companies than other data minimization laws because it allows companies to collect or use personal data if they "can demonstrate a compelling reason" that is "in the best interest of children," Cal. Civ. Code § 1798.99.31(b)(3), while other laws do not offer such an exception.

Second, the law prohibits certain uses of personal information. *Id.* § 1798.99.31(b)(1) (prohibiting *use of personal information* the company knows, or has reason to know, causes "material detriment" to children);

---

[5] https://epic.org/a-proposed-compromise-the-state-data-privacy-and-protection-act/.

*id.* § 1798.99.31(b)(4) (prohibiting *use of personal information* for purpose unrelated to reason it was collected unless in best interest of child); *id.* § 1798.99.31(b)(8) (limiting *use and retention of personal information* collected for age estimation). For example, the prohibition against profiling by default in Section 1798.99.31(b)(2) prevents companies from automatically using children's personal information to predict their behavior or other personal characteristics. This prohibition protects against the harm caused to children when their *personal information* is used to target them with ads and other content. Companies do not *need* to profile users to show them content. This is also a *default* setting, so the law allows users to choose when a company can profile them for, e.g., content presentation purposes, instead of leaving the choice entirely in the companies' hands. Some companies are already offering such options to users in Europe as part of their compliance with the Digital Services Act. Meta, for instance, says that it will give users the option to view and discover content through means other than Meta's "AI ranking and recommendation processes." Nick Clegg, *New Features and Additional Transparency Measures as the*

*Digital Services Act Comes Into Effect*, Meta (Aug. 22, 2023).[6] Users will be able to choose to view content "only from people they follow, ranked in chronological order, newest to oldest" and their search results will be based "only on the words they enter, rather than personalised specifically to them based on their previous activity and personal interests." *Id.*

Third, the law prohibits companies from using manipulative design techniques, commonly referred to as "dark patterns," that subvert users' wishes to enrich companies. Fed. Trade Comm'n, *Bringing Dark Patterns to Light* 3 (2022).[7] Dark patterns trick or annoy users so that the users act in the company's interest, such as divulging more personal information than they otherwise would. The AADC prohibits companies from using dark patterns to induce users into providing more personal information than they otherwise would or to use dark patterns to take any other action that would lead to a "material detriment" identified in their assessment. Cal. Civ. Code §

---

[6] https://about.fb.com/news/2023/08/new-features-and-additional-transparency-measures-as-the-digital-services-act-comes-into-effect/.
[7] https://www.ftc.gov/reports/bringing-dark-patterns-light.

1798.99.31(b)(7). An example of the latter would be "nudging" kids to turn profiling on by bombarding them with pop-ups on a daily basis asking them if they want to turn profiling on to improve their user experience. Another example of a dark pattern would be making the option to turn profiling on simple and prominent, while making it much more difficult to deactivate profiling. Prohibiting dark patterns has no impact on the content users can access. Dark patterns are methods companies use to control user behavior. Eliminating dark patterns *enhances* user control and thus can only enhance user access to information.

Finally, the AADC includes requirements for a company to signal when the company or a parent is collecting or tracking certain information. *Id.* § 1798.99.31(b)(6), (a)(8). It also contains several transparency and reporting requirements. *See id.* §§ 1798.99.31(a)(3)–(4), (a)(7), (a)(9), (a)(10). None of these impact access to content in any conceivable way.

Limiting the collection and use of personal information does not limit users' access to content. Companies do not need unfettered access to users' personal information to make content available to users, and

they certainly do not need to amass the detailed behavioral profiles they currently do. The AADC limits some of the power companies currently have to dictate the conditions under which users access content on their platforms. Limiting companies' power over how users access content can only *enhance* user access to information by making it easier for them to see what *they* want to see, not just what the companies want them to see.

## II. THE AADC HAS A FLEXIBLE, RISK-BASED AGE ESTIMATION OPTION, NOT A STRICT AGE VERIFICATION REQUIREMENT.

To ensure that child users receive the AADC's heightened privacy protections, the law gives companies two options. One option is to give all users heightened privacy protections, which guarantees that children receive the necessary protections. Cal. Civ. Code § 1798.99.31(a)(5). The other option is to estimate the age of users to a level of certainty proportionate to the risk level identified in the DPIA and then to apply the heightened privacy protections to the users the company estimates to be children. *Id.* The AADC does not require companies to *verify* the age of their users: it explicitly requires only an *estimate*. The strength of the estimate is also dependent on the risk the

company finds that the service poses to kids' privacy. Thus, age estimation under the AADC is not one-size-fits-all. The lower the risk the service poses to kids' privacy, the less certain companies need to be about the ages of their users.

There are several methods available to companies to estimate age. These methods ensure varying levels of certainty depending on how the company implements the method. The general categories of age estimation methods include self-attestation, parental controls, and using data the company already collects.

*Self-Attestation*

One form of age estimation is self-attestation. Many businesses already rely on self-attestation to estimate whether a user is of a certain age or within an age range for COPPA compliance, among other purposes. Fed. Trade Comm'n, *Complying with COPPA: Frequently Asked Questions* (July 2020).[8] The mechanism is fairly simple: when a user attempts to access an online service or product or open an account,

---

[8] https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.

a business asks the user to enter their birthdate or check a box saying that they are within a certain age range. The amount of data collected through self-attestation is minimal, in stark contrast to age verification methods.

While there are ways to circumvent self-attestation requests, there is reason to believe that users would not attempt to do so in the context of AADC compliance. Companies request the age of users under the AADC so that they can give kids heightened privacy protections, not to exclude them from the service. If companies explain to kids that they are asking their age so that they can give them greater privacy protections, not to stop them from using the service, kids would have less reason to lie about their age. *See* 5Rights Foundation, *But How Do They Know It Is a Child?* 10 (2021).[9]

Including various levels of "friction," or design elements that have the effect of slowing a process, can also give businesses greater certainty that self-attestations are accurate. Many businesses currently

---

[9] https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf.

design their self-attestation process with limited friction, allowing user to immediately enter another birth date or age if the initial age submitted was under the desired age threshold. Businesses can add friction to a self-attestation method by requiring users to wait a day, a week, or another appreciable amount of time before changing or entering a new a birth date. A business could also add an additional element of certainty on top of a self-attestation procedure by providing an effective mechanism for parents to request that their kids' accounts be removed or suspended because they are under 18 years of age.

*Parental oversight*

Another way businesses can estimate users' ages is by enlisting the help of parents. Businesses can recognize flags or signals from device-level, user-level, or platform-level parental control settings to inform their age estimation. Most internet users access internet content via Windows, Android or MacOS/iOS systems, and through one of three web browsers: Chrome, Safari or Firefox. Parents can set parental control settings for their children on any of these major operating systems and internet browsers. *See* David Nield, *How to Use Parental Controls in Your Google, Apple, and Microsoft Account*, Wired (Nov. 8,

2020).[10] Device-level parental controls are also widely available on tablets, smartphones, video game consoles and computers. *See* Clare Stouffer, *How to Set Parental Controls on Every Device: An Absolutely Ultimate Guide*, Norton (Sept. 29, 2022).[11] Age estimation based on device-flags is privacy-protective because it does not require additional data collection beyond what parents have already provided about their child's age through parental controls.

*Existing data*

Many of the businesses the AADC regulates can, and already do, use the data they collect about users to estimate their age. *See* Erica Finkle et al., *How Meta Uses AI to Better Understand People's Ages on Our Platforms*, Meta (June 22, 2022);[12] Sarah Perez, *TikTok CEO Says Company Scans Public Videos to Determine Users' Ages*, TechCrunch (Mar. 23, 2023).[13] Businesses often infer age for advertising purposes.

---

[10] https://www.wired.com/story/parental-controls-google-apple-microsoft-account/.
[11] https://us.norton.com/blog/how-to/how-to-set-parental-controls.
[12] https://tech.facebook.com/artificial-intelligence/2022/06/adult-classifier/.
[13] https://techcrunch.com/2023/03/23/tiktok-ceo-says-company-scans-public-videos-to-determine-users-ages/.

*See* Nico Grant et al., *YouTube Ads May Have Led to Online Tracking of Children, Research Says*, N.Y. Times (Aug. 17, 2023).[14] If companies can estimate age to deliver ads, they can estimate age to give kids greater privacy protections.

A recent federal complaint filed by a coalition of 33 Attorneys General against Meta illustrates the extent to which companies are already using the data they collect to estimate users' ages. The complaint alleges various COPPA violations based on findings that Meta has "actual knowledge" of Instagram and Facebook users under 13 years of age. Compl. ¶¶ 642-811, *California et al. v. Meta Platforms, Inc. et al.*, 4:23-cv-05448 (N.D. Cal. Oct. 24, 2023).[15] The complaint alleges that Meta gathered the information used to estimate age through different sources and processes, like parental reporting, market penetration measurements, and age-modeling algorithms that are

---

[14] https://www.nytimes.com/2023/08/17/technology/youtube-google-children-privacy.html.
[15] https://oag.ca.gov/system/files/attachments/press-docs/Less-redacted%20complaint%20-%20released.pdf.

trained to analyze the content of posts and other cues to determine age. *See id.*

Businesses can also use third-party data to estimate whether a user is a child. For example, a business that works with a third-party company that already provides a service like security screenings or marketing analytics can use or repurpose the third-party data about users to estimate age. Age estimation based on existing data that the business has (or has access to through a third-party) would not require additional data collection and could be tailored to achieve various levels of certainty based on the type of data used.

*Age Verification Not Required*

Finally, even if a company finds that the risk their service or product poses to kids is very high, there is never a circumstance where the company is required under the AADC to verify age. The AADC requires estimation of age, it does not require an actual "verification" process. In fact, because the AADC's DPIA provision requires companies to consider potential privacy risks when selecting an age estimation method, *see* Cal. Civ. Code § 1798.99.31(a)(1)(A)–(B), and specifically whether the method will require the company to "collect[] or

process[] sensitive personal information of children, *id.* § 1798.99.31(a)(1)(B)(viii), the DPIA would counsel *against* ever implementing invasive age verification methods. Invasive age verification likely also violates the AADC's data minimization mandate, as the data collection required for age verification is not necessary to estimate age. *Id.* § 1798.99.31(b)(3). Instead of implementing invasive age verification, a company that finds that their product or service poses a high risk to kids' privacy should either redesign their product or service to be safer for children or apply heightened privacy protections to all users.

## III. THE AADC IS DISTINGUISHABLE FROM KIDS' ONLINE SAFETY LAWS PASSED IN OTHER STATES BECAUSE IT DIRECTS COMPANIES TO INCLUDE KIDS IN ONLINE SPACES SAFELY, NOT TO EXCLUDE THEM AND OTHERS THROUGH PRIVACY-INVASIVE DATA COLLECTION.

As California considered and passed the AADC, other states—namely, Texas, Utah, and Arkansas—enacted legislation with superficially similar characteristics that have led to unfair comparisons among the laws. All of the laws purport to ensure kids' safety online

and treat kids differently than adult users. But that is where the similarities end.

First, while the AADC allows companies to use flexible methods to evaluate whether users are kids so that they can be given more privacy protections than adults, the other states direct companies to block child users from accessing some or all of their services. Second, the AADC allows companies to estimate users' ages with data they already have or through non-invasive methods such as self-attestation. Other states' laws require companies to verify users' ages using privacy invasive data collection that could discourage even adult users from accessing the service. Finally, the AADC does not require age estimation *at all* if a company applies strong privacy protections to all users.

First, the Texas, Utah, and Arkansas laws direct companies to exclude kids from online spaces or to block specific categories of content. All of these laws create barriers to *access*, either through age verification alone or in combination with parental consent. The Texas Securing Children Online through Parental Empowerment Act, for instance, requires companies to "register" the age of all users and to block known minor users from accessing certain categories of content.

H.B. 18, 88th Leg., Reg. Sess. (Tex. 2023) (to be codified at Tex. Bus. & Com. Code §§ 509.001–509.051, 509.053(a)). It also requires companies to verify the age of "any person seeking to *access* content" on services where more than one-third of the content is "harmful material or obscene" and bars such companies from entering into any "agreement with [a minor] for *access*" to the service. *Id.* §§ 509.057(a)–(b) (emphasis added). The Arkansas Social Media Safety Act requires companies to verify the age of users "before allowing *access* to the social media companies' social media platform," S.B. 396, 94th Gen. Assemb., Reg. Sess. (Ark. 2023), § 4-88-1102(c)(1) (emphasis added), and prohibits social media companies from allowing minors to have accounts on their services unless they have parental consent, *id.* § 4-88-1102(a). The Utah Social Media Regulation Act, like the Arkansas law, requires social media companies to "verify the age" of new and existing social media account holder, to "not permit" minor users on their platform without parental consent, and to "deny *access*" to account holders who fail to verify their age. S.B. 152, 65th Leg., Reg. Sess. (Utah 2023), §§ 13-63-102(1), (3)(a), (3)(b).

The AADC, on the other hand, does not create barriers to *access*. Companies are not directed to exclude children—or any other users—from their services under any conditions. Instead, companies are allowed to include children, but must give them (or all users) strong privacy protections. In other words, the AADC directs companies to use age estimation not to bar access to their services but to identify users who must receive strong privacy protections.

As explained in Section I above, the AADC also does not require companies to block *any* content; it only requires companies to assess how their use of kids' personal information could expose them to harmful content and, at most, requires them to alter how they are *using kids' personal information* to deliver such content to kids, not to stop delivering the content to them altogether.

Comparing the AADC's DPIA provision to the Texas content-blocking provision illustrates the difference between the AADC's approach, which seeks to remedy the specific harm caused by use of personal information to target content to kids, and the Texas law, which seeks to block kids' access to certain types of content. The Texas content-blocking provision does not mention personal information at all;

it instead directs companies to "prevent the known minor's exposure" to several categories of content. H.B. 18 § 53(a). The law also requires companies to "creat[e] a comprehensive list of harmful material" to "block" such content from child users, *id.* § 53(b)(1)(A); "us[e] filtering technology" to "block[] material," *id.* § 53(b)(1)(B); and to use hash technology and other methods to "identify recurring harmful material," *id.* § 53(b)(1)(C). The AADC includes no such requirements.

Second, the Texas, Utah, and Arkansas laws require covered companies perform invasive age verification on all users, while the AADC gives companies the option to use data they already have or other non-privacy-invasive methods to estimate age. In Texas, if more than one-third of the content a companies' service hosts is "harmful material or obscene," they must "use a commercially reasonable age verification method to verify" that the user is over 18 years of age. *Id.* § 509.057(a). The Arkansas law requires social media companies "use a third-party vendor to perform reasonable age verification" which includes providing "a digitized identification card," "government-issued identification," or "any commercially reasonable age verification method." S.B. 396 § 4-88-1102(c)(1)–(2). The Utah law requires

companies to "verify the age" of users but leaves the specification of acceptable methods to an agency rulemaking. S.B. 152 §§ 13-63-102(3)(a), (4).

As explained in Section II above, the AADC does not require companies to *verify* users' ages at all; it gives companies the option to *estimate* users' ages. Estimation is necessarily less exacting than verification. Estimation only requires a best guess, while verification requires an ascertainment of truth. *See* 5Rights Found., *supra*, at 6. Indeed, verifying which users are children necessarily means verifying which users are not, which is why laws requiring age verification also impose privacy costs on adult users. While the Texas, Arkansas, and Utah laws require companies to perform invasive verification of all users, the AADC allows companies to use data they already collect, signals from parental control software, or non-invasive data collection methods like self-attestation, to estimate users' ages. Such age estimation methods are unlikely to discourage users from accessing services because the users are either unlikely to know they are occurring or the request for information will not be considered onerous.

The AADC also does not draw arbitrary lines between what online services require age estimation and which do not, such as the Texas law's one-third harmful content rule. Under the AADC, age estimation confidence levels are based on risk, and risk is based on how companies choose to use kids' personal data. If a company finds that their use of kids' personal data creates such a high risk that they need to collect additional data to estimate users' ages to the required level of confidence, the company can change the way they use kids' data, lower the risk to kids, and lower the confidence level required for age estimation.

Finally, the AADC does not require *any* company use age estimation at all. Every company has the option of giving all users strong privacy rights instead of estimating the age of users. Cal. Civ. Code § 1798.99.31(a)(5). Thus, if a company determined that they were incapable of estimating users' ages to the required level of certainty or that their users would protest their use of a particular kind of age estimation method, the company could simply provide all users with strong privacy protections. As explained in Section I above, applying

such privacy protections to adult users would not limit their access to information.

In sum, the AADC is easily distinguishable from laws passed in other states. Those laws create barriers to access content and services; the AADC does not impact access, it provides kids with strong privacy protections so that they can access services safely. The other states' laws require invasive data collection that may discourage adults from accessing services; companies can comply with the AADC by using data they already have or through non-invasive data collection. And while the other states require companies to verify users' ages, the AADC gives companies the option to forgo age estimation altogether.

## IV. COMPARING THIS CASE TO *RENO V. ACLU* SHOWS WHY THE AADC IS CONSTITUTIONAL.

The district court's First Amendment analysis in this case focused on the risk that adults will lose access to content online as a result of companies' compliance with the data protection requirements in the AADC. This argument is essentially an extension of the central premise of the Supreme Court's decision in *Reno v. ACLU*, 521 U.S. 844 (1997), but the district court failed to consider the dispositive factors in *Reno*.

Comparing the AADC to the Communications Decency Act of 1996 ("CDA") provisions at issue in *Reno* is instructive because while the laws are superficially similar, the CDA was clearly a kind of content-based, speech-chilling statute that the AADC is not.

In *Reno v. ACLU*, the Supreme Court evaluated the constitutionality of CDA provisions that blocked any website operator or user from showing inappropriate content to minors. The CDA criminalized the act of showing children "indecent" or "patently offensive" communications. *Reno*, 521 U.S. at 849. This prohibition applied to anybody on the internet, whether they were a private person, a nonprofit, a corporation, or an educational institution. *See* 47 U.S.C. §§ 223(a), (d) (1994 ed., Supp. II). And it imposed criminal penalties, including potential imprisonment, for violations of the Act. *Id.* The Court found that the CDA violated the Constitution because it was a facially vague, overbroad, content-based criminalization of speech.

The Supreme Court found that the CDA was facially vague because, in different provisions, it prohibited showing "indecent" and "patently offensive" materials without providing a definition of those terms or explanation of how they related to each other. The Court noted

that these "ambiguities" in the linguistic descriptions of the prohibited speech "will provoke uncertainty among speakers about how the two standards relate to each other and just what they mean." *Reno*, 521 U.S. at 870–71.

The *Reno* Court noted that vagueness in the CDA was especially problematic because its restrictions were content-based. Vague, content-based restrictions have an "obvious chilling effect on free speech." *Id.* at 871–72 (citation omitted) . The Court explained that vague resolutions pose a "risk of discriminatory enforcement" that offends the Constitution. *Id.* at 872.

The CDA's content-based nature and vagueness was especially problematic because the statute imposed criminal penalties on offenders. The Court explained that the "opprobrium and stigma" of a criminal conviction, and the potential jailtime, "may well cause speakers to remain silent rather than communicate even arguably unlawful words, ideas, and images." *Id.* at 872. It noted that criminalizing speech "poses greater First Amendment concerns than those implicated by" civil regulations. *Id.*

It was this combination—vagueness tied to criminal punishment based on content—that worried the *Reno* Court. The combination of the three factors brought an "increased deterrent effect" on the exercise of speech rights. *Id.* at 872. The Court feared that important discussions, such as those about "birth control practices, homosexuality, . . . or the consequences of prison rape," would be chilled. *Id.* at 871. And it noted that these provisions would provide any internet user with a heckler's veto: By claiming that speech with which one disagrees is offensive or indecent and that one's minor child read it, a person could threaten others with criminal prosecution. *Id.* at 880. The Court found that these features, taken together, meant that the CDA had not "been carefully tailored to the congressional goal of protecting minors from potentially harmful materials." *See id.* at 871.

Because of the speech-chilling dangers inherent in vague, content-based statutes, the *Reno* Court insisted that the CDA could not "be justified if it could be avoided by a more carefully drafted statute." *Id.* at 874. It found that the statute failed to meet this standard because it would suppress a large number of legal adult-to-adult communications. *See id.* In the Court's view, there was no effective way to verify users'

ages, so companies would inevitably need to restrict speech among adults for fear that one participant in a conversation might actually be a child. *See id* at 876. The Court also criticized the CDA for imposing its requirements on every internet user instead of focusing on specific types of speakers such as corporations. It compared the statute unfavorably to those it upheld in cases such as *Ginsberg v. New York*, 390 U.S. 629 (1968) and *FCC v. Pacifica Foundation*, 438 U.S. 726 (1978), which limited their reach "to commercial speech or commercial entities." *Id.* at 877. By contrast, the CDA's "open-ended prohibitions embrace all nonprofit entities and individuals." *Id.* The Court illustrated the worrying overbreadth of these provisions by describing how "a parent allowing her 17-year-old to use the family computer to obtain information on the Internet that she, in her parental judgment, deems appropriate could face a lengthy prison term." *Id.* at 878. Because the law cut so broadly, and because the Government could not explain why a less restrictive provision would not be equally as effective in protecting children, the Court found that the CDA was not narrowly tailored and was thus unconstitutional. *See id.* at 879.

The AADC does not resemble the CDA. First, it does not have the trifecta of traits that worried the *Reno* Court and led it to hold the CDA to a high standard of tailoring. Also, its flexible, tailored statutory provisions mean that even if the AADC limited user access to content, it would be unlikely to result in the suppression of speech among adults.

Unlike the CDA, the AADC is not vague, content-based, or enforced through criminal penalties. Instead of prohibiting companies from showing children vaguely defined categories of content, it regulates how companies collect, manage, and use children's data. *See supra* Part I.A. A company may still provide any of the same kinds of content that it did before the AADC was enacted—it simply can't use a child's data to specifically target that child with types of content if the company assesses that it could be harmful or that such targeting would create a risk of "material detriment" to children. Additionally, the AADC, unlike the CDA, imposes only civil penalties, which means it does not involve the "increased deterrent effect" and "greater First Amendment concerns" that the CDA did by imposing criminal penalties.

The AADC avoids the CDA's constitutional overbreadth issues by more narrowly and logically regulating specific entities. The CDA

applied to anyone who sent or displayed a message on the internet, *see* 47 U.S.C. §§ 223(a), (d) (1994 ed., Supp. II), whereas the AADC applies only to large commercial entities that trade in personal information, *see* Cal. Civ. Code § 1798.140(d) (incorporated into the Act through §1798.99.30(a)), and that are "likely to be accessed by children," *id.* § 1798.99.31(a), (b). This is the kind of careful targeting that the *Reno* Court called for in its overbreadth analysis and criticized the CDA for lacking. *See Reno*, 521 U.S. at 877.

The AADC also avoids the CDA's constitutional overbreadth issues because it does not require invasive age verification. The CDA criminalized any instance of showing offensive or indecent materials to children online but provided an affirmative defense for those who "restrict [children's] access by requiring certain designated forms of age proof, such as a verified credit card or an adult identification number." *Id.* at 860–61. The government argued that this defense precluded the Court's overbreadth worries because websites could simply distinguish between children and adults. *Id.* at 880. But the Court rejected that argument because the government could not prove that these age verification methods were technologically or commercially feasible. *Id.*

at 881–82. The affirmative defense was no defense at all given the difficulty of accurate age verification, and the Court "refused to rely on unproven future technology to save the statute." *Id.* at 882. The AADC, by contrast, implements a much more flexible standard that is satisfied if companies *estimate* users' ages or forego age estimation altogether by extending strong privacy rights to all users. *See* Cal. Civ. Code § 1798.99.31(a)(5). This is not a large lift: companies already engage in age estimation through a combination of self-attestation, device control, and analyzing existing profile data. *See supra* Section II. This scheme avoids the constitutional overbreadth issues that age verification raised in the context of the CDA.

## CONCLUSION

For the foregoing reasons, EPIC respectfully urges the Court to reverse the district court's order granting NetChoice's motion for a preliminary injunction.

**Date:** December 20, 2023

/s/ Megan Iorio
Megan Iorio
Tom McBrien
Suzanne Bernstein
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

*Attorneys for Amicus Curiae Electronic Privacy Information Center*

## CERTIFICATE OF COMPLIANCE

I am the attorney or self-represented party.

**This brief contains 6,976 words,** excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief *(select only one)*:

[ ] complies with the word limit of Cir. R. 32-1.

[ ] is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.

[X] is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).

[ ] is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.

[ ] complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:

[ ] it is a joint brief submitted by separately represented parties;

[ ] a party or parties are filing a single brief in response to multiple briefs; or

[ ] a party or parties are filing a single brief in response to a longer joint brief.

[ ] complies with the length limit designated by court order dated _____.

[ ] is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

**Signature:** */s/ Megan Iorio* **Date:** December 20, 2023

## CERTIFICATE OF SERVICE

I certify that on December 20, 2023, this brief was e-filed through the CM/ECF System of the U.S. Court of Appeals for the Ninth Circuit. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

**Date:** December 20, 2023

/s/ Megan Iorio
Megan Iorio
Tom McBrien
Suzanne Bernstein
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

*Attorneys for Amicus Curiae*
*Electronic Privacy Information Center*