No. 25-2366

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-BLF
The Honorable Beth Labson Freeman, District Court Judge

BRIEF OF COMMON SENSE MEDIA AS *AMICUS CURIAE* IN SUPPORT OF DEFENDANT-APPELLANT

Ariel Fox Johnson
DIGITAL SMARTS LAW &
POLICY, LLC
16781 Chagrin Blvd. #536
Shaker Heights, OH 44120
(216) 309-2689
ariel@dslpconsulting.com

Attorney for Amicus Curiae
Common Sense Media

June 17, 2025

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1, *amicus curiae* Common Sense Media 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*

Common Sense Media ("Common Sense") is a nonpartisan, nonprofit organization dedicated to improving the lives of kids and families by providing the trustworthy information, education, and independent voice they need to thrive.[1] Common Sense has been studying children and teens' relationships with social media and technology, and the impacts of such relationships, for over a decade. For example, Common Sense has recently detailed how social media can amplify pressure and stress teens feel along a variety of metrics (e.g. achievement, appearance, friendship), how children and teens struggle to set healthy boundaries with technology (including missing sleep) given constant notifications from apps and the pull of devices, and how more teens view features like location sharing and public

[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 or submission of this brief. No person, other than *amicus curiae* or its counsel, contributed money intended to fund the preparation or submission of this brief.

accounts negatively vs. positively.[2] Common Sense has also studied age assessment, publishing a whitepaper last fall considering the current landscape of age assurance, technologically, legislatively, and in industry practice, and examining ways to develop age assurance practices and rules that are privacy protective, proportionate, fair, and equitable—and that satisfy U.S. constitutional concerns.[3]

Common Sense has advocated for policy solutions at the state and federal level that would help enable a digital world where all kids can thrive. Common Sense was a co-sponsor of the California Age-Appropriate Design Code Act (CAADCA).[4] Based on Common Sense's years of experience, both in terms of understanding technology's effects

---

[2] *See* Our Research Program, Common Sense Media, https://www.commonsensemedia.org/research, (last updated Mar. 24, 2025).

[3] *See* Ariel Fox Johnson, *U.S. Age Assurance Is Beginning to Come of Age: The Long Path Toward Protecting Children Online and Safeguarding Access to the Internet,* Common Sense Media (2024), https://www.commonsensemedia.org/sites/default/files/featured-content/files/2024-us-age-assurance-white-paper_final.pdf.

[4] *See* Cal. Sen. Jud. Comm. Analysis, The California Age-Appropriate Design Code Act (2022), https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=202120220AB2273.

on children and in developing legislative proposals to protect them online, *amicus* believes that design codes like the CAADCA help ensure children are protected in the digital world. And Common Sense believes that these codes, focused on product features and privacy protections, and not on access to content and services, offer protective approaches consistent with the First Amendment. This includes the CAADCA's requirement to "[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*." Cal. Civ. Code § 1798.99.31(a)(5) (italics added). Ultimately, Common Sense's interest is ensuring that this Court's judgment about the CAADCA, and specifically the age estimation provisions, is based on a thorough understanding of the current landscape of technology, regulation, and children's experiences.

SUMMARY OF THE ARGUMENT

The district court erred in holding that NetChoice was likely to succeed in its claim that the age estimation provision is unconstitutional. The age estimation provision of the CAADCA is not

facially invalid under the First Amendment. The district court rested its decision on two misunderstandings: that the purpose of age estimation under CAADCA is to determine what "content" is appropriate, and that age estimation would "require" the collection of "private information." Dist. Ct. ECF No. 143 at 36-37. First, there are a variety of *reasons* to estimate age—and here, the statutory reason does not relate to content or limiting access to content. Second, there are a wide and growing variety of *ways* to estimate age, including ones that do not "require businesses to collect private information that users may not wish to share." Dist. Ct. ECF No. 143 at 37. There is no record, as required under *Moody v. NetChoice, LLC*, 144 S. Ct. 2383 (2024), from which the district court could have assessed the full range of age estimation techniques, which types of age estimation NetChoice's members challenge, or even who those members are.

The district court misunderstood the purpose of age estimation and mistakenly held—despite the plain statutory text—that age estimation under the CAADCA would force businesses to make content choices. Age estimation can take many forms and may be used for many purposes, not all of which include limiting access to content.

Under the CAADCA, age estimation is for the purpose of providing privacy protections and other data use protections. *See* Cal. Civ. Code § 1798.99.31(a)(5). Age estimation for the purpose of providing higher privacy—as is the case here—does not in and of itself regulate speech.

The remaining relevant constitutional question is whether age estimation might otherwise impermissibly chill speech, for example because it could impede access to content. This is a highly fact dependent question based on the specifics of the age estimation and entity doing the estimating. The district court erred in its assessment here as well. The district court mistakenly, and without sufficient record evidence, found that age estimation under the CAADCA would require businesses to collect information users did not want to share. Importantly, not all forms of age estimation require collecting any additional information. New privacy-protective ways to estimate age are announced with increasing speed. Further, with the CAADCA, the California legislature intentionally drafted a privacy-protective age estimation requirement.

The Supreme Court articulated a high bar for facial challenges under *Moody*. Specifically, it required that courts evaluating facial

challenges must consider "a law's full set of applications," which is a rigorous statute- and fact-specific inquiry, especially in the age estimation context. *Moody*, 144 S. Ct. at 2394. With respect to age estimation, there must be a detailed record, and this record must address with specificity different age estimation methods permitted or prescribed, the purposes of age estimation, the burdens they may impose on users, and whether this would deter access. Only after considering a detailed factual record could the district court determine whether or not the CAADCA and specifically its age estimation provision would "prohibit[] a substantial amount of speech relative to its plainly legitimate sweep." *Moody,* 144 S. Ct. at 2409. Here, there was no such detailed record, and certainly no sufficient record upon which to find that age estimation under the CAADCA would "require" the collection of "private information" or that sites make any changes to content. Respectfully, the district court decision should be reversed.

ARGUMENT

I. AGE ESTIMATION UNDER THE CAADCA IS NOT FOR PURPOSES OF DETERMINING CONTENT, AS THE DISTRICT COURT MISTAKENLY HELD

The CAADCA is a content-neutral privacy and design law. It is therefore distinct from laws that use age assurance to allow or disallow access to content and services. Indeed, most historical and modern cases involving age assurance have been the opposite, and specifically about using age assurance for access to content like social media or pornography. References to decades-old *Reno v. ACLU,* 521 U.S. 844 (1997) and *Ashcroft v. ACLU,* 542 U.S. 656 (2004) are not on point, as they do not squarely address or consider whether and when age assurance in a content-neutral law constitutes a constitutional burden. In *Reno* and *Ashcroft* the Court looked to the specific (and very different) facts underlying those cases and the then current age assessment technology and ramifications of its use. Those cases did not squarely address or consider whether and when age assurance in a content-neutral law constitutes a constitutional burden. They also considered age estimation technology as it existed decades ago. Thus, they are not factually useful. But in terms of legal approach, they

considered the technology carefully and demanded a well-developed factual record. *See Reno* at 876-877 (considering effectiveness of age determination following a trial on the merits); *Ashcroft* at 672 (relying on extensive factual findings at district court level and insisting lower court update factual findings on remand). The CAADCA is a different law, for different purposes–and it deserves its own well developed factual record. It is also a very different law than modern efforts in other states to restrict access to social media sites and the content there. *See, e.g.*, *NetChoice, LLC v. Griffin*, No. CV 23-05105, 2023 WL 5660155, at *1, *3 (W.D. Ark. Aug. 31, 2023); *NetChoice, LLC v. Reyes*, 748 F. Supp. 3d 1105, 1114-15 (D. Utah 2024), appeal docketed, No. 24-4100 (10th Cir. Oct. 11, 2024); *NetChoice v. Yost,* No. 24-CV-00047, 2025 WL 1137485 (S.D. Ohio Apr. 16, 2025).

Age estimation under the CAADCA is not for purposes of adjusting, limiting access to, or in any way affecting content. Indeed, as this Court has previously noted, age estimation here does not clearly trigger First Amendment scrutiny in all or even most applications. *NetChoice, LLC v. Bonta*, 113 F.4th 1101, 1122-23 (9th Cir. 2024) (citations omitted). Under the CAADCA, age estimation is

for the purposes of providing "privacy and data protections." Cal. Civ. Code § 1798.99.31(a)(5). It is not, as the district court found without statutory explanation, for the purposes of providing "content… appropriate for that age." Dist. Ct. ECF No. 143 at 36. Age estimation here does not on its own implicate speech—it does not require companies who choose to assess age to block access to content or services, for either children or adults. And companies who choose not to implement age assurance at all are instead simply to apply strong "privacy and data protections" to everyone—which also does not require blocking access to content or services for either children or adults. *See* Cal. Civ. Code § 1798.99.31(a)(5). "Privacy" and "data protections," the statutory terms, are widely used in law; the CAADCA is itself an effort to further privacy under the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020.[5] Privacy here addresses how businesses collect, use, and share

[5] Cal. Civ. Code §§1798.100-199, *amended* by Cal. Civ. Code §§1798.99.28-1798.99.40 (2024).

personal information about individuals.[6] The term "data protection", which is used often internationally, encompasses the similar concept about protection of an individuals' "personal data."[7]

Under the CAADCA, if companies do not wish to assess age, they do not need to—and this does not mean that they need to sanitize or clean-up their websites' content. The statute requires that sites and services covered must: "Estimate 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." Cal. Civ. Code § 1798.99.31(a)(5). The statute does not say that if companies choose not to provide age estimation, content must be "sanitized" or "only child-appropriate" as the district court mistakenly believed. Dist.

---

[6] *California Consumer Privacy Act (CCPA)*, State of California Department of Justice, https://oag.ca.gov/privacy/ccpa (last updated Mar. 13, 2024).

[7] The European Union General Data Protection Regulation "lays down rules relating to the protection of natural persons with regard to the processing of personal data." Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), L 2016 O.J. (L 119) 1, 32.

Ct. ECF No. 143 at 36, 38. Companies who do not wish to age estimate could have whatever content they wish so long as they have strong privacy and data protections in place by default, thereby applying the "privacy and data protections afforded to children to all consumers" as required under the statute. Cal. Civ. Code § 1798.99.31(a)(5). Indeed, such a site may be quite desirable to adults, as they may be afforded a measure of privacy not otherwise available to them. While companies could comply with the CAADCA by offering high privacy protections across the board, often, companies resist protecting privacy for all audiences as a default because they believe that less privacy protective features lead to more profits. But it is ultimately up to the company.

II. THE DISTRICT COURT LACKED A NECESSARY RECORD TO ASSESS WHETHER AGE ESTIMATION WOULD REQUIRE THE FORCED COLLECTION OF PRIVATE INFORMATION AND ANY RECORD AS TO HOW AGE ASSURANCE OCCURS IN PRACTICE

It was error for the district court to find that age estimation under the CAADCA would require the forced collection of private information. This is especially true given the paucity of the record, which did not demonstrate how age assurance would occur for NetChoice's different members in any level of detail.

This Court has previously held that the age estimation provision of the CAADCA and other provisions, "on their face, do not necessarily impact protected speech in all or most applications," and that "[a]s in *Moody,* the record needs further development to allow the district court to determine 'the full range of activities the law covers.'" *NetChoice, LLC v. Bonta*, 113 F.4th at 1122-23. (citations omitted). As age does not trigger a bar to access, the question is whether undergoing the age estimation method itself will have the effect of substantially deterring access. This is a highly fact-specific question, based on the nature of the age estimation used and the type of service itself. It requires considering the current state of technology and the variety of means of assessing age, as well as the variety of services users are accessing. Following *Moody*, this Court held that the record before the district court was insufficient to determine whether the age estimation requirement of the CAADCA facially violated the First Amendment

NetChoice yet once again brought essentially a facial challenge against age estimation, and it once again did not provide a detailed record that would enable any court to properly assess this challenge, offering no specific applications of the standard let alone the full scope

of applications for its members. Nonetheless, the district court mistakenly determined that there was only one specific way to comply with the age estimation provision, "collect[ing] private information that users may not wish to share", and that the "practical effect of the CAADCA's age estimation requirement is that businesses will gather and create 'a trove of sensitive data regarding children.'" Dist. Ct. ECF No. 143 at 37. The district court failed to follow the guidance of this Court and *Moody* by determining—on a very sparse record—that there was only one way to comply with age estimation. It did not consider the full range of options available, nor did NetChoice's few member declarations on age estimation offer specifics about how they conducted age estimation, or whether they implemented age estimation at all. For example, NetChoice's declarations offered on remand—after it had been told it had an insufficient record—merely claimed that the CAADCA would require them to "collect far more private data from its readers than it does now" or that the CAADCA would "inevitably require the collection of private information." Masnick Supp. Decl. ¶ 7 (Dist. Ct. ECF No. 101-5), Paolucci Supp. Decl. ¶ 6 (Dist. Ct. ECF No. 101-6). Further, even were the declarations to offer specifics about

their own services and planned age estimation practices—which they did not—these declarations from only a few sites would not be a sufficient record on which to facially invalidate the age estimation provisions in their entirety. *See Moody,* 144 S. Ct. 2397-98 *(*criticizing parties for focusing on only a few applications of the statute and ignoring many other sites, services, and applications).

Indeed, it is not even clear that the declarants are not already compliant with the CAADCA's alternative to assuring age proportionate to risks—which is to provide a high level of default privacy to all users. Cal. Civ. Code § 1798.99.31(a)(5). For example, both Techdirt and Dreamwidth support "anonymous" users on their sites and Paolucci explains that Dreamwidth is "committed" "to respecting the privacy" of its users. Masnick Supp. Decl. ¶ 7 (Dist. Ct. ECF No. 101-5), Paolucci Supp. Decl. ¶ 6 (Dist. Ct. ECF No. 101-6). Masnick additionally says Techdirt has a "deliberate practice to minimize how much data we collect and retain about our readers." Masnick Decl. ¶ 1 (Dist. Ct. ECF No. 101-5). These companies could already be compliant with CAADCA's age estimation requirements if

they provide a high level of privacy and data protections to all users, with no age assurance actions required.

As discussed below, age estimation does not need to be privacy invasive, and the district court was incorrect in finding—especially on such a limited record—that age estimation would necessarily require the forced collection of private information. *See* Dist. Ct. ECF No 143 at 37. Age estimation may take many technical forms. Multiple of these forms do not require the transmission or collection by a service of "private information." Since the constitutionally relevant question is whether specific age estimation practices may deter adults from accessing specific content or services, the details of such age estimation practices matter. NetChoice failed to identify the full scope of specific age estimation practices that sites and services would take, and it was therefore impossible for the district court to analyze the scope of age estimation provisions under the CAADCA (step one in a First Amendment facial challenge), let alone which applications may violate the First Amendment and how those measure up against the rest (step two). *See X Corp v. Bonta,* 166 F.4th 888, 899 (9th Cir. 2024).

III. AGE ESTIMATION CAN OCCUR IN A VARIETY OF WAYS, WHICH ARE CONSTANTLY INCREASING, AND WHETHER ESTIMATION POSES ANY CONSTITUTIONAL CONCERNS IS HIGHLY FACT DEPENDENT

Age estimation can and will occur in a variety of ways, especially given the variety of sites and services that exist, each with their unique and different data practices. Estimation does not require, as the district court erroneously concluded, the forced collection of information "users may not wish to share." Dist. Ct. ECF No. 143 at 37. Companies themselves, like NetChoice member Google, are publicly announcing ways to assess age that do not require the additional collection of personal data when users access new sites and services.[8] Google is enabling a digital wallet solution whereby users can securely indicate age to everything from dating apps to healthcare to rideshares. In late February, Apple also announced "a new privacy-

---

[8] *See, e.g.*, Alan Stapelberg, *It's Now Easier to Prove Age and Identity with Google Wallet*, The Keyword, (Apr. 29, 2025), https://blog.google/products/google-pay/google-wallet-age-identity-verifications/; *Helping Protect Kids Online*, Apple (Feb. 2025), https://developer.apple.com/support/downloads/Helping-Protect-Kids-Online-2025.pdf.

protective way for parents to share their kids age range" with apps.[9] As Apple explained, "Parents will now have the ability to share their child's age range with the apps they use while protecting their child's privacy." Specifically, Apple will make it easy for parents to share age range (without sharing sensitive information like birth date): "families can have age-appropriate experiences within apps without the App Store collecting unnecessary sensitive personal data on every user."[10]

The CAADCA is not overly prescriptive in its age assessment requirements, and is drafted to accommodate changing technology. It states that "[a]ge assurance shall be proportionate to the risks and data practice of an online service, product, or feature" and that companies undertaking it should "estimate the age of child users with a reasonable level of certainty appropriate to the risks." Cal. Civ. Code § 1798.99.31(a)(5), (b)(8).

---

[9] Apple, *supra* note 8 at 4.
[10] *Id.*

Current methods of assessing age include attestation (where a user or parent provides their own age or age range), approximating (where companies use data points to approximate a user's age), and age verification (which typically verifies a user's age against an ID or hard identifier). These methods carry different privacy implications and can provide different levels of friction. Friction in design can be a delay or a barrier to use, and it may be miniscule or substantial.[11] Friction does not necessarily increase as one moves from simpler to more complicated forms of age assurance. A simple form of age assessment includes attestation, where a user states an age or range. Approximation is in the middle and can be done based on data a service already holds (such as a user's online behavior on the platform, or their social graph on social media) or may be done by cross-referencing other data such as transactional data.[12] It may also be done

---

[11] *See* Brett Frischmann & Susan Benesch, *Friction-in-Design Regulation as a 21st Century Time, Place, and Manner Restriction*, 25 Yale J. L. & Tech. 376, 379 (2023), https://yjolt.org/sites/default/files/frischmann_benesch.friction-in-design_regulation.376.pdf.

[12] Fox Johnson, *supra* note 3 at 7.

via biometric information, such as facial or voice assessments.[13] Techniques like facial scans typically place a user in an approximate age range using their facial features, they do not determine exact age. Scans to estimate age are not scans to biometrically identify an individual like the facial scans now common before boarding a flight; age estimation scans do not process sufficient information to identify an individual, but rather "can estimate users' ages without storing identifiable biometric data."[14] Scans also need not be of faces—indeed, cutting-edge technology can use AI and machine learning to determine age with high accuracy "by having the user move just his hand in front

---

[13] *Id.* at 8; *see* Nat'l Inst. of Standards and Tech., Face Analysis Technology Evaluation: Age Estimation and Verification 43 (2024); Sarah Forland et al., *Age Verification: The Complicated Effort to Protect Youth Online*, New America Foundation Open Technology Institute, at 10-12 (2024), https://d1y8sb8igg2f8e.cloudfront.net/documents/Age_Verification_The_Complicated_Effort_to_Protect_Youth_Online_2024-04-22_165_bS2AcQ5.pdf.

[14] Luke Hogg & Evan Swartztrauber, *On the Internet: No One Knows You're a Dog: Examining the Feasibility of Privacy-Preserving Age Verification Online*, Foundation for American Innovation, at 12 (Feb. 18, 2025), https://cdn.sanity.io/files/d8lrla4f/staging/0287856bc4be1f8a80271e3e9048e48920f41f7b.pdf.

of a camera."[15] Such biometric estimation can occur "with no recording of the individual ever being stored or, in many instances, ever leaving the user's device."[16] This means such scans do not pose the same security or privacy risks. A final form of age assurance is age verification—which is on a spectrum next to approximation and may also include verification via banking or credit card details—that typically uses a hard identifier like a government ID.[17] Attestation, approximation, and verification can all be designed in ways that increase or that minimize friction for a user.

Privacy-protective methods of age assurance exist today and will continue to expand in the coming weeks, months, and years. Privacy-protective methods of age estimation may make use of third-party verifiers, zero knowledge proofs, and decentralized and device-based learning. In addition, age assurance can occur in the background and on already collected data, without users needing to take any additional steps.

---

[15] *Id.* at 13.
[16] *Id.*
[17] Fox Johnson, *supra* note 3 at 10.

For example, age assurance, either attestation, approximation, or verification, may make use of a third-party verifier. Using a third-party verifier is a privacy-protective recommendation of France's data protection agency.[18] A third-party verifier could be a private, a state or federal entity, or an independent, quasi-governmental, or non-profit organization established for this purpose. It could be a device or app store that has received an attestation of age. As noted above, Apple recently announced it will offer a Declared Age Range Application Programming Interface (API) within its app store ecosystem, a "narrowly tailored, data-minimizing, privacy-protective tool to assist app developers" that "gives kids the ability to share their confirmed age range with developers, but only with the approval of their parents."[19] As Apple explains, "[t]his protects privacy by keeping parents in control of their kids' sensitive personal information, while

---

[18] Noah Apthorpe et al., *Online Age Gating: An Interdisciplinary Evaluation*, at 26 (Aug. 1, 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4937328.
[19] Apple, *supra* note 8 at 5.

minimizing the amount of information that is shared with third parties."[20]

Third-party verifiers can pass information on to the site or service that requires age assurance—and this information may be very limited. It is possible to design "double blind" systems, in which verifiers do not know which sites or services a user is accessing, and sites and services do not know details about who is accessing their site, only that users meet verification criteria. Information may be passed through "zero knowledge proofs" that do not do anything other than indicate to the service requesting the verification that the user is confirmed to meet or not meet the age criteria.

"Zero knowledge proofs" are a privacy protective way to assure age. Zero knowledge proofs "allow a user to verify some fact about themselves without giving up any information other than that the fact is true."[21] The district court expressed skepticism that such proofs are widely available to covered businesses in the U.S. *See* Dist. Ct. ECF No

---

[20] *Id.*
[21] Hogg & Swartztrauber, *supra* note 14 at 11.

143 at 37. But zero knowledge proofs are not theoretical—"[i]ntroduced in the 1980s but refined throughout the 2000s, ZKPs [zero knowledge proofs] have become more practical for real world applications thanks to increased computation power, improvements in algorithms, and the emergence of blockchain and other distributed computing technologies."[22] Indeed, "[t]hese advancements have made ZKPs an ideal tool for addressing privacy concerns" for age assessment.[23] And, importantly, NetChoice's own member companies are using zero knowledge proofs for the purpose of age assurance. For example, Google explained in April that it was offering "Fast and private age verification."[24] Specifically, Google explained:

> "Given many sites and services require age verification, we wanted to develop a system that not only verifies age, but does it in a way that protects your privacy. We are integrating Zero Knowledge Proof (ZKP) technology into Google Wallet, further ensuring there is no way to link the age back to your identity. This implementation allows us to provide speedy age verification across a wide range of mobile devices, apps and websites"[25]

---

[22] *Id.*
[23] *Id.*
[24] Stapelberg, *supra* note 8.
[25] *Id.*

With respect to ZKP, Google specifically noted that "To help foster a safer, more secure environment for everyone, *we will also open source our ZKP technology to other wallets and online services*." (emphasis added).[26] ZKP technology is part of reality for U.S. companies, not a fictional futuristic concept.

Another way privacy can be enhanced when conducting age estimation is by having the estimation take place on-device or in-browser. Decentralized frameworks such as blockchains and other distributed technologies avoid centralized repositories of data and allow processing of any information to occur on a user's device, protecting privacy and limiting security and data breach risks.[27] These methods will not expose users to the same privacy or security risks as assurance that takes place on a vendors' servers. There will be no centralized database subject to hacking risks, which the district court expressed fears over. *See* Dist. Ct. ECF No. 143 at 37. By limiting information passed to companies and websites to just whether a user

---

[26] *Id.*
[27] Hogg & Swartztrauber, *supra* note 14 at 12.

meets an age criteria or not, such methods minimize the data privacy risk by minimizing the amount of data stored and [28]

Lastly, in general and as discussed above, age estimation can be designed in ways such that any personal information remains on a user's device, and that all that is sent to a service like one of NetChoice's members is a signal of an age, or a signal that a user meets a given age threshold.

Another way age estimation can operate without requiring the collection or sharing of additional personal information is when companies assess age via already-collected data. This assurance can happen in the background, without requiring onerous steps on the part of the user. Indeed, many companies regulated by the CAADCA are likely already able to estimate age of users based on existing data. Google has announced it will begin testing a machine-learning based age estimation model.[29] Reportedly, "[the] age estimation model

---

[28] *See* Apthorpe et al., *supra* note 18 at 24-26.
[29] Jen Fitzpatrick, *New Digital Protections for Kids, Teens and Parents*, The Keyword (Feb. 12, 2025), https://blog.google/technology/families/google-new-built-in-protections-kids-teens/.

will use existing data about users, including the sites they visit, what kinds of videos they watch on YouTube, and how long they've had an account to determine their age."[30] Meta is developing ways to identify accounts that belong to teens that would run in the background and be invisible to users.[31]

Further, to the extent companies are already estimating age based on existing data in order to serve users ads, companies could use those estimates to comply with the CAADCA. And companies *do* estimate age for monetization purposes. Meta, for example, has had internal charts boasting penetration into 11-12 year olds. The company maintained separate "modified" "estimated" or "imputed" ages of children, based on its algorithmic modeling, for most purposes like improving "engagement" and revenue, and then a different "stated age"

---

[30] Emma Roth, *Google Will Use Machine Learning to Estimate a User's Age*, The Verge (Feb. 12, 2025, 12:00 PM), https://www.theverge.com/news/610512/google-age-estimation-machine-learning.

[31] *Introducing Instagram Teen Accounts: Built-In Protections for Teens, Peace of Mind for Parents*, Meta, https://about.fb.com/news/2024/09/instagram-teen-accounts/ (last updated June 11, 2025, 1:30 PM).

for legal purposes under children's privacy law.[32] In such a scenario, it seems likely no additional information from a user would be required to assess age—the company already collected and processed it sufficiently to have made an assessment.

Ultimately, there are a variety of different ways age estimation can take place. Age estimation methods can be burdensome to a user, or barely noticeable. They could implicate privacy in large ways, or in very little ways. As demonstrated above, it is entirely possible that the service estimating age receives no information from the user other than that a user's age is ok or not ok; that no "private" information needs to leave a user's device; or that a user can use a third party verifier and never again take another action because that verifier will

---

[32] Complaint for Injunctive & Other Relief at ¶ 732-37, People of the State of California v. Meta Platform Inc., No. 4:23-cv-05448-YGR (N.D. Cal. Nov. 23, 2023), https://oag.ca.gov/system/files/attachments/press-docs/Less-redacted%20complaint%20-%20released.pdf; *see also* Nico Grant et al., *YouTube Ads May Have Led to Online Tracking of Children, Research Says*, N.Y. Times (Aug. 17, 2023) https://www.nytimes.com/2023/08/17/technology/youtube-google-children-privacy.html.

signal age and nothing more through zero knowledge proofs, and one age assessment signal can be used across the web.

IV. THE LEGISLATURE INTENTIONALLY SET UP A PRIVACY PRESERVING SYSTEM FOR AGE ESTIMATION

It is possible to assess age in ways that preserve privacy and minimize data collection. And, with the CAADCA, the California Legislature intentionally set up such a privacy-preserving system. First, the CAADCA is explicitly not a statute that requires "age verification" (the word verification does not appear, and "establish," which was in the originally introduced bill was later replaced with "estimate"), rather, it speaks of "estimation" and "assurance." *Compare* A.B. 2273, 2021-2022 Leg., Reg. Sess. (Cal. 2022) (as introduced on Feb. 16, 2022) with Cal. Civ. Code § 1798.99.31(a)(5). In addition, it is a proportional rule—tying the certainty of the assessment to the risks inherent in the company's existing data practices. Cal. Civ. Code § 1798.99.31(b)(8). This demonstrates that the Legislature did not want companies to use privacy invading technologies, and that, in the tradeoff between privacy and certainty, the Legislature clearly wanted companies to choose privacy at the expense of certainty. Third, the

Legislature additionally sought to ensure privacy was respected in the text of the CAADCA, by providing that data collected for age estimation may not be retained any longer than necessary to determine age and may not be used for any other purposes. Cal. Civ. Code § 1798.99.31(b)(8).

Companies should therefore not be subjecting users to privacy risks for age assurance purposes if those risks are beyond the risks companies' data practices already present to users. NetChoice's members which offer "anonymous" experiences do not need to collect any further data about users and can maintain anonymity. (This is in contrast to NetChoice's social media members, who already collect and maintain age information, including sometimes already government ID.) If use of an age assurance method presented heightened privacy risks compared to the privacy risks from that companies' existing data practices, in order to be compliant with the CAADCA the company should not be using this age assurance method—the method would not be appropriate considering the baseline level of risk. Many companies already collect a vast amount of data on their users, so if the company can already assess age based on existing data, then that is how the

company should assess age. If a company poses extremely low privacy risks, and they know nothing about their users, then they should use an extremely minimal form of age estimation. The fact that the certainty level of estimation should increase with the risk of the underlying data practices shows the Legislature's understanding that the more data a company collects about users, the more likely they are to be able to estimate age to a greater level of certainty based on that data to start.

V. THE DISTRICT COURT ERRED IN FINDING NETCHOICE MET ITS BURDEN FOR A PRELIMINARY INJUNCTION

Age estimation under the CAADCA is not a choice "between intruding into user privacy… or publishing only child-appropriate content" Dist. Ct. ECF No. 143 at 38. No privacy needs to be intruded (and certainly no more privacy than businesses like social media sites currently intrude), and no child-appropriate content needs to be published.

Whether age-based rules for privacy implicate speech is highly dependent on the specific age estimation tools used, the entity doing the age estimation, services' pre-existing data practices and information about their users, and the purpose of age estimation.

These are all factual questions. NetChoice did not provide any specifics about how any services would implement age estimation under CAADCA, let alone provide the full set of applications of age estimation that this Court held was required in order to make a determination about the constitutionality of such measures. Instead, NetChoice repeated yet again its facial claims. Unfortunately, the district court simply accepted NetChoice's broad, speculative statements—for example that services may respond by "requiring even adults to relinquish personal information." Dist. Ct. ECF No. 101 at 20.

The Supreme Court has cautioned that "facial challenges threaten to short circuit the democratic process by preventing duly enacted laws from being implemented in constitutional ways." *Moody,* 144 S. Ct. at 2397 (internal citations omitted). In an era when parents and caregivers are clamoring for more protections for young people online, the California Legislature duly enacted a thoughtful law that can be implemented in constitutional ways. NetChoice's speculation should not short circuit this democratic process.

CONCLUSION

For the foregoing reasons, Common Sense respectfully urges this Court to reverse the district court's order.

Date: June 17, 2025

s/ Ariel Fox Johnson
Ariel Fox Johnson
DIGITAL SMARTS LAW & POLICY, LLC
16781 Chagrin Blvd. #536
Shaker Heights, OH 44120
(216) 309-2689

Attorney for Amicus Curiae Common Sense Media

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(g), I certify:

1. This brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(5) because it contains 6,307 words, excluding the items exempted by Fed. R. App. P. 32(f).

2. The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6) because it has been prepared in a proportionally spaced typeface, Century Schoolbook, in size 14-point font

Date: June 17, 2025

/s/ Ariel Fox Johnson
Ariel Fox Johnson

Attorney for Amicus Curiae Common Sense Media

CERTIFICATE OF SERVICE

I certify that on June 17, 2025, this brief was e-filed through the ACMS System of the U.S. Court of Appeals for the Ninth Circuit. I certify that all participants in the case are registered ACMS users and that service will be accomplished by the ACMS system.

Date: June 17, 2025

s/ Ariel Fox Johnson
Ariel Fox Johnson
DIGITAL SMARTS LAW & POLICY, LLC
16781 Chagrin Blvd. #536
Shaker Heights, OH 44120
(216) 309-2689

Attorney for Amicus Curiae Common Sense Media