No. 25-146

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

NetChoice, LLC,
Plaintiff-Appellant

v.

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

On Appeal from the United States District Court for the Northern District of California
No. 5:24-cv-07885-EJD
The Honorable Edward J. Davila, District Court Judge

BRIEF OF COMMON SENSE MEDIA AS *AMICUS CURIAE* IN SUPPORT OF DEFENDANT-APPELLEE AND AFFIRMANCE

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

March 6, 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 detailed how social media can amplify pressure and stress teens feel along a variety of metrics (e.g. achievement, appearance, friendship) and how children and teens struggle to set healthy boundaries with technology (including missing sleep). As part of its efforts into understanding effective ways to protect youth online, Common Sense has studied age assessment. For example, Common Sense published a whitepaper considering the

---

[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.

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. Common Sense has also assessed parents' relationships with their children's technology and common areas of frustration and helplessness. Recently, Common Sense reported on media use among 0-8 year olds, including how frequently parents of such children were likely to use tools to manage screen time.

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 supported the Protecting Our Kids From Social Media Addiction Act (SB976), as well as a similar law in New York, where rulemaking is currently underway. Based on Common Sense's years of experience, both in terms of understanding technology's effects on children and in developing legislative proposals to protect them online, *amicus* believes that product safeguards addressing addictive features, like SB976, help ensure children can thrive in a digital world. Further, efforts focused on product features, and not on access to

content and services, offer protective approaches consistent with the First Amendment. Combining such efforts with carefully crafted regulations assessing age enables laws to protect youth while reflecting the latest state of evolving technology. Ultimately, Common Sense's interest is ensuring that this Court's judgment about SB976, and specifically the age assurance provisions, is based on a thorough understanding of the current landscape of technology, regulation, and families' experiences.

SUMMARY OF THE ARGUMENT

The district court correctly held that age assurance in SB976 was not ripe for consideration.

In this brief, *Amicus* will explain how technological developments offer an ever-increasing number of methods of age assurance, which may be used for a variety of purposes. These methods pose different constitutional considerations, and most are able to survive constitutional scrutiny.

In particular, there are ways to assess age that do not require the collection of additional personal information. Further, any concerns about specific forms of age assurance are appropriately raised during the rulemaking consultation, which has not yet commenced.

In addition, users are not currently "anonymous" on most or all of Netchoice's member companies' platforms. So, it cannot be assumed that any age assurance would lessen any supposed "anonymity" currently enjoyed on platforms governed by SB976. This claim of anonymity itself requires a highly factual inquiry into each site or service's current information collection practices. Additionally, SB976 requires that any information collected for age assurance be used only

for the purpose of age assurance and deleted immediately after it has been used to determine the user's age. These are higher protections than for much information currently collected.

Amicus will also explain how protections like SB976's, which are on by default and tailored to the addictive features of platforms, are so critical to parents. This is because other alternatives are insufficient.

As demonstrated by the Supreme Court's recent consideration of *Free Speech Coalition, Inc. v. Paxton,* age assurance is not per se unconstitutional. And, under longstanding Supreme Court case law, including *Reno* and *Ashcroft,* assessing the constitutionality of age assurance is a highly fact intensive issue. There is no factual record here, nor could there be given the age assurance regulations have not yet been promulgated.

ARGUMENT

I. THERE ARE AN INCREASING VARIETY OF WAYS AND REASONS TO ASSESS AGE, ALL OF WHICH POSE DIFFERENT CONSTITUTIONAL CONSIDERATIONS

SB976 does not set forth specific requirements or methods of reasonably determining age. Rather, it requires that after January 1, 2027, companies must "[r]easonably determine[] that the user is not a

minor, including pursuant to regulations promulgated by the Attorney General." Cal. Health & Safety Code § 27001(a)(1)(B). The Attorney General must adopt "regulations regarding age assurance" in the interim. § 27006(b). Age assurance can occur in a variety of ways. Which method or methods the Attorney General will detail is unknown, because the Attorney General has not yet concluded or even commenced the age assurance rulemaking.

"Age assurance" encompasses a broad category of age determination techniques that estimate age to varying levels of certainty.[2] Age assurance is distinct from "age verification", which is a narrow subset of assessing age and "which confirms user age with a high level of certainty—often through collecting a user's sensitive personal information."[3] Importantly, techniques that estimate age to a

---

[2] 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 5-11 (Sept. 30, 2024), https://www.commonsensemedia.org/sites/default/files/featured-content/files/2024-us-age-assurance-white-paper_final.pdf.

[3] *Helping Protect Kids Online*, Apple 5 (Feb. 2025), https://developer.apple.com/support/downloads/Helping-Protect-Kids-Online-2025.pdf.

lower level of certainty do not require the same level of data collection and processing as age verification techniques, and so do not present the same privacy, security, or access risks. Whether age-based rules implicate speech is dependent on the specific age assurance tools used, the entity doing the age assurance, services' pre-existing data practices and information about their users, and the purpose of age assurance.

There are ever-evolving ways to assess age, and there will be even more by January 1, 2027. Many of these age assurance techniques prioritize privacy. Also, age assurance as contemplated in SB967 does not require companies to collect more information than they already have. Approved age assurance methods under SB976 are likely to be just as capable—if not more capable—of preserving "anonymity" as current data practices of business that utilize addictive-feeds. Moreover, recommendations about specific aspects or applications of age assurance are most appropriately raised during rulemaking.

A. There are constantly evolving ways to assess age, including a number of privacy protective ones

Age assurance is a fast-moving space, both in terms of technology and regulations. Experts have noted that technological advancements,

especially in artificial intelligence and biometrics, "have led to a booming diversity of techniques" for age assurance.[4] Indeed, seemingly daily, there are reports of new methods or initiatives regarding age assurance, including from NetChoice's members. For example, in mid February, Google announced it will begin testing a machine learning age estimation model.[5] In late February, Apple announced "a new privacy-protective way for parents to share their kids age range" with apps.[6] It is hard to predict what the technology will look like later this month, let alone next year, or in 2027.

Current methods of assuring age include attestation (where a user or parent provides their own age or age range), approximating (where

---

[4] 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 12 (Feb. 18, 2025), https://www.thefai.org/posts/on-the-internet-no-one-knows-you-re-a-dog.

[5] Jen Fitzpatrick, *New digital protections for kids, teens, and parents,* Google: The Keyword (Feb. 12, 2025), https://blog.google/technology/families/google-new-built-in-protections-kids-teens/.

[6] Apple, *supra* note 3 at 4; Miranda Nazzaro, *Apple unveils 'age assurance' technology amid child safety push*, The Hill (Feb. 28, 2025, 11:17 AM), https://thehill.com/policy/technology/5168887-apple-age-assurance-technology/.

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.[7] Friction does not necessarily increase as one moves from simpler to more complicated forms of age assurance. A simple form of age assurance 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.[8] It may also be done via biometric information, such as facial or voice assessments.[9] Techniques like facial scans typically

---

[7] *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.

[8] Fox Johnson, *supra* note 2 at 7.

[9] *Id.* at 8; *see* Kayee Hanaoka et al., *Face Analysis Technology Evaluation: Age Estimation and Verification,* National Institute of

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."[10] 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 of a camera."[11] Such biometric estimation can occur "with no recording of the individual ever being stored or, in many instances, ever leaving the user's device."[12] 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

---

Standards and Technology 43 (2024), https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8525.pdf.; Sarah Forland et al., *Age Verification: The Complicated Effort to Protect Youth Online,* New America Foundation Open Technology Institute, 10-12 (2024).

[10] Hogg & Swartztrauber, *supra* note 4 at 12.

[11] *Id.* at 13.

[12] *Id.*

approximation and may also include verification via banking or credit card details—that typically uses a hard identifier like a government ID.[13] Attestation, approximation, and verification can all be designed in ways that increase or that minimize friction for a user.

B. Age assurance can exist in ways that do not require companies to collect additional personal or sensitive information, and that do not require additional steps from users

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 assurance 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.

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

---

[13] Fox Johnson, *supra* note 2 at 10.

protection agency.[14] A third-party verifier could be a private entity, 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. 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."[15] As Apple explains, "[t]his protects privacy by keeping parents in control of their kids' sensitive personal information, while minimizing the amount of information that is shared with third parties."[16]

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

---

[14] Noah Apthorpe et al., *Online Age Gating: An Interdisciplinary Evaluation*, 26 (Aug. 1, 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4937328.
[15] Apple, *supra* note 3 at 5.
[16] *Id.*

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."[17] Such proofs are acknowledged by NetChoice's *amicus* as a way for "individuals to confirm they meet an age threshold, without disclosing their exact date of birth or other personal information." Center for Democracy and Technology, Amicus Br. 21. They are then dismissed as "a theoretical solution" posing "resource challenges." *Id.* at 22-23. 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

---

[17] Hogg & Swartztrauber, *supra* note 4 at 11.

to increased computation power, improvements in algorithms, and the emergence of blockchain and other distributed computing technologies."[18] Indeed, "[t]hese advancements have made ZKPs an ideal tool for addressing privacy concerns" for age assessment.[19]

Another way privacy can be enhanced when conducting age assurance is by having the age assurance 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.[20] Such methods do not expose users to the same privacy or security risks as assurance that takes place on vendors' servers.

By limiting information passed to companies and websites to just whether a user meets an age criteria or not, such methods minimize

---

[18] *Id.*
[19] *Id.*
[20] *Id.* at 12.

the data privacy risk by minimizing the amount of data stored and disclosed.[21]

Another way age assurance 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 SB976 are likely already able to estimate age of users based on existing data. Google recently announced it would begin testing a machine-learning based age estimation model.[22] Reportedly, "[the] age estimation model 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."[23] Meta is developing ways to identify accounts

---

[21] *See* Apthorpe et al., *supra* note 14 at 24-26.
[22] Fitzpatrick, *supra* note 5.
[23] 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.

that belong to teens that would run in the background and be invisible to users.[24]

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 SB976. 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" for legal purposes under children's privacy law.[25] No additional information or from a user was required—the company already assessed age.

---

[24] *Introducing Instagram Teen Accounts: Built-In Protections for Teens, Peace of Mind for Parents*, Meta (Sept. 17, 2024), https://about.fb.com/news/2024/09/instagram-teen-accounts/.

[25] Complaint for Injunctive and 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.

Ultimately, there are a variety of different ways age assurance can take place. Age assurance 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 assessing age under SB976's not-yet-existent age assurance regulations receives no information from the user other than that a user's age is ok or not ok; that no "private" or sensitive 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 signal age and nothing more through zero knowledge proofs, and one age assessment signal can be used across the web.

C. Any age assurance methods under SB976 can preserve anonymity at least as much as NetChoice's members' current business practices do

There is no factual record from which to assume SB976's future age assurance regulations will burden users' rights to be anonymous. First, as discussed above, there are numerous and growing privacy protective methods to assess age, including those that collect and/or share no additional information about users. For example, double-blind processes can "ensure that neither the platform requesting verification

nor the verification provider knows the user's identity of online activities."[26] Second, it is highly questionable whether any users are currently "anonymous" on most or all of NetChoice's member companies' services regulated by SB976. Indeed, in its current appeal, NetChoice is challenging the ability to as a default use addictive-feeds—feeds that only exist when users are *not* anonymous, as such feeds are by definition "based in whole or in part, on information provided by the user, or otherwise associated with the user or the user's device." § 27000.5(a). By definition, it seems that a platform with actually anonymous users would not be able to show them addictive-feeds. And NetChoice has provided no factual record to demonstrate otherwise.

Rather, what facts we do know about companies with such feeds are that the user experience is far from anonymous. Large social media platforms make huge profits by tracking users' every interaction with their platforms, as well as following them elsewhere around the

---

[26] Hogg & Swartztrauber, *supra* note 4 at 20.

internet, creating intricate profiles that intentionally can be used to identify individuals.[27] For example, in a 2023 lawsuit of dozens of states against Meta, alleging that Meta designed and deployed harmful features on Instagram and Facebook to addict children and teens, company statements highlight the business model is based on ad targeting. "In terms of our ability to continue to grow the advertising business, it's about working to develop the best—the best products we can to enable advertisers to achieve their end business results. Targeting obviously very is [sic] important in that."[28] Targeting, by definition, requires information about the targeted user.

---

[27] *See* Electronic Privacy Information Center, Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem, epic.org 1, 36–38, 61–62 (2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf.

[28] Complaint for Injunctive and Other Relief at ¶ 55, People of the State of California v. Meta Platform Inc., *supra* note 25.

A recent complaint against TikTok from the Massachusetts Attorney General cites a lengthy list of information TikTok collects from users, per its own privacy policy.[29] This includes:

> "account information"…"User-generated content, including comments, photographs, livestreams, audio recordings, videos, text, hashtags, and virtual item videos that [the user] choose[s] to create with or upload to the Platform ("User Content") and the associated metadata, such as when, where, and by whom the content was created"), "Information [the user] share[s] through surveys or [their] participation in challenges, research, promotions, marketing campaigns, events, or contests such as [their] gender, age, likeness, and preferences."

Tiktok's policy states it also "automatically collects certain information" from users when they use its platform:

> "including internet or other network activity information such as [a user's] IP address, geolocation-related data, unique device identifiers, browsing and search history (including content [a user] ha[s] viewed in the Platform), and Cookies" … ""Image and Audio Information," i.e.,"information about the videos, images and audio that are a part of your User Content, such as identifying the objects and scenery that appear, the existence and location within an image of face and body features and attributes, the nature of the audio, and the text of the words spoken in your

---

[29] Complaint and Jury Demand at ¶ 77-78, Commonwealth of Massachusetts v. TikTok Inc., No. 2484-cv-2638-BLS-1 (Mass. Super. Ct. Feb. 3, 2025), https://www.mass.gov/doc/tiktok-complaint-unredacted/download.

> User Content" which TikTok uses "for demographic classification, [and] for content and ad recommendations."[30]

Surely, such users are not anonymous at present. The British privacy regulator, the Information Commissioner's Office (ICO), who has been intensely studying this issue, just announced an investigation into TikTok's use of personal information of teenagers to make recommendations and deliver suggested content to their feeds.[31] The ICO also noted, "[w]e have concerns about the volume and range of children's personal information that these systems use, and whether they have sufficient protections in place for children."[32]

Further, the text of SB976 indicates a desire to protect users' privacy in assessing age. SB976 directs the Attorney General to adopt

---

[30] *Id.*

[31] *Investigations announced into how social media and video sharing platforms use UK children's personal information*, ICO (Mar. 3, 2025), https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/02/investigations-announced-into-how-social-media-and-video-sharing-platforms-use-uk-children-s-personal-information/.

[32] *Children's code strategy progress update – March 2025*, ICO (2025), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/protecting-childrens-privacy-online-our-childrens-code-strategy/children-s-code-strategy-progress-update-march-2025/.

regulations regarding "age assurance"—not "age verification" that can require substantially more personal information. § 27006(b). The Legislature additionally sought to ensure privacy was respected by requiring that any information collected for age assurance "shall not be used for any purpose other than compliance with this chapter or with another applicable law" and that information collected shall be deleted immediately after it is used to determine a user's age…except as necessary to comply with state or federal law." § 27001(b). These purpose specification and deletion requirements are likely stronger than other requirements that govern the personal information companies currently collect.

Ultimately, to understand whether any age assurance practices required by SB976 would actually lessen any supposed anonymity on platforms governed by SB976 would require a highly factual inquiry into each site and service's current information collection, use, and retention practices, and comparison to whatever regulations are promulgated. This requires both the regulations—which do not exist—and a detailed factual record about specific services' practices—which NetChoice has failed to build.

D. Suggestions about specific age assurance mechanisms are more appropriately raised during rulemaking

NetChoice's *amici's* concerns about how some forms of age assurance are more effective, or more privacy protective, than others, or recommendations about ways to safeguard information involved in age assurance, are more appropriately raised to the Attorney General during the rulemaking. So too are concerns about how to address potential mis-classified adults (who might then not see an addictive feed until they turn it on). In California, the Office of Administrative Law ensures agencies comply with California's Administrative Procedure Act.[33] In a regular rulemaking, there are "comprehensive public notice and comment requirements."[34] This "comprehensive process is intended to further the goal of public participation."[35] There will be ample time to recommend preferred age assurance mechanisms by the public, industry, civil society, and other experts. As the district

---

[33] *Rulemaking Process*, Ca. OAL, https://oal.ca.gov/rulemaking_process/.
[34] *Regular Rulemaking Process*, Ca. OAL, https://oal.ca.gov/rulemaking_process/regular_rulemaking_process/.
[35] *Id.*

court correctly observed, SB976's regulations can interpret "reasonable" age assurance efforts in many ways. The court correctly noted that age assurance could operate in the background and require no user input, or it could permit covered entities to use information they already collect for advertising profiles. There is ample space for the Attorney General to adopt privacy-protective, constitutional regulations regarding age assurance.

II. PROTECTIONS LIKE SB976 ARE CRITICAL BECAUSE OTHER ALTERNATIVES ARE INSUFFICIENT FOR FAMILIES

Contrary to NetChoice's assertions, research shows that parents do not feel they are able to adequately supervise their children's online experiences, or that current tools are sufficient. According to a 2023 Mott Children's Hospital National Poll on Children's Health, the top three concerns for parents were: overuse of devices/screen time, social media, and internet safety—ahead of other issues like healthcare costs,

school violence, and smoking.[36] Parents are dissatisfied with the current state. The Supreme Court Justices' questioning at oral argument in *Free Speech Coalition v. Paxton* recently reinforced this, with Justices repeatedly stating filtering does not work.[37]

Parents find current tools difficult and overly burdensome. In a recent Pew Center report, only 26% of parents say it's easy to manage how much time their children spend on their phone.[38] Qualitative research has found that "amongst non-users of parental controls there was a widespread lack of engagement with this technology. This was

---

[36] *Mott Poll Report: Overuse of devices and social media top parent concerns,* M.S. Mott Children's Hospital (Aug. 21, 2023), https://mottpoll.org/reports/overuse-devices-and-social-media-top-parent-concerns.

[37] Transcript of Oral Argument at 9-10, 12, *Free Speech Coalition, Inc. v. Paxton,* No. 23-1122 (U.S. Jan. 15, 2025), https://www.supremecourt.gov/oral_arguments/argument_transcripts/2024/23-1122_7m58.pdf (Justice Alito: "There's a huge volume of evidence that filtering doesn't work. We've had many years of experience with it."; Justice Barrett: "… let me just say that content filtering for all those different devices, I can say from personal experience, is difficult to keep up with.").

[38] Monica Anderson et al., *How Teens and Parents Approach Screen Time*, Pew Research Center (Mar. 11, 2024), https://www.pewresearch.org/internet/2024/03/11/how-teens-and-parents-approach-screen-time/.

driven by a combination of '[t]he perception, particularly amongst parents with lower levels of confidence about technology, that the process of selecting and installing parental controls was complex and time-consuming.'"[39]

Common Sense's research demonstrates that few parents therefore engage with such tools, though more make efforts as children get older and presumably are using screens more independently. Common Sense's 0-8 report found that three-quarters (75%) of parents whose children use screen media do not use any tools or settings to limit screen time. Parents of older children (age 5 to 8) are more likely to use tools to manage screen use than those with very young children (younger than 2). For example, 30% of parents of older children use software to limit screen time.[40]

---

[39] *Parents' views on parental controls*, Jigsaw Research 9 (Oct. 2012), https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/children/oct2012/annex_1.pdf?v=333782#page=5.13.

[40] *The Common Sense Census: Media Use by Kids Zero to Eight*, Common Sense 1, 29 (2025), https://www.commonsensemedia.org/sites/default/files/research/report/2025-common-sense-census-web-2.pdf.

What's more, many of the parental control tools available that NetChoice references, such as tools to control devices and websites, do not offer the protections of SB976, or offer them only in a blunter, more expansive way that could limit expression. For example, SB976 targets the specific feature of the addictive-feed, but still allows children by default to access all content. Other parental tools referenced do not. In addition, SB976 would be on by default, unlike other tools which require a parent to set them up. This lack of protection by default is a critical shortcoming, given that many parents find current tools too time-intensive.

III. GIVEN THE FACT-SPECIFIC INQUIRY REQUIRED TO CONSIDER AGE ASSURANCE, THE MULTITUDE OF AGE ASSURANCE OPTIONS, AND THE LACK OF REGULATIONS, IT IS BOTH PREMATURE AND IMPOSSIBLE TO CONSIDER THE AGE ASSURANCE PROVISIONS HERE

The district court correctly held that age assurance in SB976 was not ripe for consideration. Age assurance is not per se unconstitutional. *See, e.g., Free Speech Coalition, Inc. v. Paxton,* No. 23-1122 (2024), *Reno v. ACLU*, 521 U.S. 844 (1997), and *Ashcroft v. ACLU*, 542 U.S. 656 (2004).

As detailed above, there are numerous ways in which to assess age, and they grow on an almost daily basis. This makes it impossible for NetChoice to develop the necessary factual record, which in turn makes it impossible for this Court to consider the constitutionality of the age assurance provisions. *See Moody v. NetChoice, LLC,* 144 S. Ct. 2383 (2024) (facial challenges require a robust factual record). The Supreme Court has repeatedly assessed age assurance provisions in an intensely factual manner. 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). Multiple decades later,

this Court is confronted with both a different law, and vastly different age assurance technology.

It is also critical to understand the operation and ramification of age mechanisms required by the laws at issue. NetChoice keeps relying on laws which are unlike SB976. Such laws require verification of user ages (requiring a high level of certainty of age), or require such verification as a condition to access to sites or services. *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*, No. CV 23-00911-RJS (CMR), 2024 WL 4135626, at *3 (D. Utah Sept. 10, 2024), appeal docketed, No. 24-4100 (10th Cir. Oct. 11, 2024); *NetChoice, LLC v. Fitch*, 738 F. Supp. 3d 753, 762 (S.D. Miss. 2024), appeal docketed, No. 24-60341 (5th Cir. July 5, 2024). SB976 neither requires verification, nor requires any type of age assurance in order for individuals to access sites or services. And it does not block access to content for minors, only to the addictive-feed feature. Further, a number of these "age verification" laws' methods were not to be clarified by regulation. *E.g., NetChoice, LLC v. Fitch*, No. CV 24-170-HSO

(BWR), 738 F. Supp. 3d 753 (S.D. Miss. 2024), appeal docketed, No. 24-60341 (5th Cir. July 5, 2024).

Whether an age assurance provision passes constitutional muster will depend on the specifics of the regulation, and the specifics of the technology, viewed in tandem with a site or service's existing practices. It is inappropriate for companies that profit from surveilling users to say age assurance, backed by sufficient privacy protections, is likely to deter such users. Given there are no regulations, and that NetChoice has failed to proffer specifics about the technology and its members' practices, the district court correctly held that the age assurance provision was not ripe for consideration.

CONCLUSION

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

Date: March 06, 2025

/s/ Ariel Fox Johnson
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

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 5,825 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: March 6, 2025

/s/ Ariel Fox Johnson
Ariel Fox Johnson

Attorney for Amicus Curiae Common Sense Media

CERTIFICATE OF SERVICE

I certify that on March 6, 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: March 6, 2025

/s/ Ariel Fox Johnson
Ariel Fox Johnson

Attorney for Amicus Curiae Common Sense Media