Alan Butler (SBN 281291)
butler@epic.org
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Avenue NW
Washington, DC 20036
Tel: 202.483.1140

Attorney for Proposed Amicus Curiae
Electronic Privacy Information Center

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

NETCHOICE, LLC, d/b/a NetChoice,

Plaintiff,

v.

ROB BONTA, ATTORNEY GENERAL OF THE STATE OF CALIFORNIA, in his official capacity,

Defendant.

Case No. 5:24-cv-07885-EJD

BRIEF OF ELECTRONIC PRIVACY INFORMATION CENTER AS *AMICUS CURIAE* IN SUPPORT OF DEFENDANT

Hearing Date: December 17, 2024
Time: 9:00 a.m.
Judge: Hon. Edward J. Davila
Court: Courtroom 4, 5th Floor

Action Filed: November 12, 2024

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes & Regulations

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 regularly participates as amicus in cases concerning the First Amendment implications of platform regulation. *See* EPIC, *The First Amendment* (2024).[2]

INTRODUCTION

The Supreme Court's decision in *Moody v. NetChoice,* 144 S. Ct. 2383 (2024), set out a rigorous standard for First Amendment challenges to platform regulations. Facial challenges must set out all potential applications of the law, assess the constitutionality of each, and weigh the constitutional applications against the unconstitutional ones. In assessing the constitutionality of each application, courts must insist on specificity. While some platform actions may be expressive, like removing or downranking messages based on a company's content guidelines, other actions, like curating feeds based on users' interactions with a site, are not evidently expressive. It is the challenger's burden to explain what specific activities, by what specific actors, are impacted by a regulation, how those activities are expressive, and how the regulation interferes with that expression.

In NetChoice's hands, though, the *Moody* decision loses all of its nuance. NetChoice insists, through broken strings of quotations, that the Court held that personalized feeds are protected expression when in fact the *Moody* Court flatly refused to make such a ruling. The majority were only willing to signal the expressiveness of one kind of curation activity: the enforcement of content moderation policies. Since SB 976 does not interfere with this activity, *Moody*'s guidance is no aid to NetChoice. In fact, SB 976 regulates exactly the curation activity whose expressiveness the Court met with skepticism: the crunching of user behavioral data to predict what content will keep a user on a platform longer.

---

[1] *Amicus* certifies that no person or entity, other than *Amicus*'s own staff or counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief, in whole or in part.

[2] https://epic.org/issues/platform-accountability-governance/the-first-amendment-and-platform-regulation/.

Instead of specifically arguing how SB 976 interferes with each regulated companies' expression, NetChoice misconstrues the Act as a ban on personalized feeds. In reality, SB 976 leaves ample room for companies to organize content and personalize feeds on their platforms. Addictive feeds are simply not necessary for the things people want to do on platforms.

The *Moody* Court's insistence on a robust factual record applies with equal force to NetChoice's challenge to the Act's age assurance provision. How age assurance will actually be implemented matters. SB 976 does not require companies to age gate their entire platforms—they can, instead, choose to age gate only the regulated features. Any potential chilling effect will also vary from tool to tool and platform to platform. There are a wide range of age assurance tools available on the market; there are likely to be even more by the time the age assurance provision takes effect in 2027. And any deterrent effect will depend on the platform that uses it—specifically, on the platform's current data and design practices. Companies that profit from invading users' privacy cannot say that age assurance, backed by sufficient privacy protections, is likely to deter users. NetChoice also cannot rely on factual findings made over twenty years ago or decisions in cases involving very different statutory requirements. NetChoice must assemble a record on age assurance, and it cannot do this until the Attorney General promulgates regulations on SB 976.

ARGUMENT

I. The addictive feeds provision does not regulate expression and leaves ample room for companies to organize and personalize feeds.

In *Moody v. NetChoice,* 144 S. Ct. 2383 (2024), the Supreme Court signaled that one specific curation practice is expressive: content moderation that reflects human value judgments about the message expressed. SB 976 does not regulate this kind of curation. The Act regulates "addictive feeds"—website features that use user behavioral data to present users with whatever content will boost their usage of a website or platform. This type of curation, called engagement maximization, "respond[s] solely to how users act online—giving them the content they appear to want, without any regard to independent content standards." *Moody,* 144 S. Ct. at 2404 n.5. Engagement-maximizing curation does not clearly express any message of the curator, and so

regulating it does not implicate the First Amendment. SB 976 leaves ample room for companies to organize and personalize content based on the messages expressed and on user choice.

Content moderation is a company's enforcement of rules about the types of content it is willing to host or promote. These rules are typically set out in companies' content moderation policies and community guidelines and enforced through teams of human moderators, with some assistance from algorithmic filtering. *See* Kate Klonick, *The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression*, 129 Yale L.J. 2418, 2423 (2020); *e.g.*, Facebook, *Community Guidelines*;[3] YouTube, *Community Guidelines*.[4] In *Moody*, the majority agreed that content moderation activities are expressive because they reflect humans' value judgments about the message expressed by the content. "When the platforms *use their Standards and Guidelines to decide* which third-party content those feeds will display, or how the display will be ordered and organized, they are making expressive choices." *Moody,* 144 S. Ct. at 2406 (emphasis added). A company that prohibits, say, pro-Nazi posts is expressing its disagreement with the message of those posts, and a law that "direct[s a company] to accommodate messages it would prefer to exclude" infringes on the company's protected editorial discretion. *Id.* at 2401.

Content moderation is distinct from engagement maximization. Maximizing for engagement means curating content in a way that maximizes the probability that a specific user will interact with a specific piece of content. *See* Arvind Narayanan, *Understanding Social Media Recommendation Algorithms*, The Knight First Amendment Institute at Columbia University 20 (2023).[5] In contrast to content moderation, which largely depends on human decision making and intervention, engagement optimization is accomplished through machine learning algorithms, called "recommendation algorithms," which essentially crunch the numbers on what will keep each user on the platform longer. *See* Ravi Iyer, *Feed Algorithms Contain*

[3] https://www.facebook.com/help/477434105621119.
[4] https://www.youtube.com/howyoutubeworks/policies/community-guidelines/.
[5] https://s3.amazonaws.com/kfai-documents/documents/4a9279c458/Narayanan---Understanding-Social-Media-Recommendation-Algorithms_1-7.pdf.

both Expressive and Functional Components, USC Neely Center for Ethics and Technology (Dec. 10, 2024).[6] The primary fuel for engagement-maximizing recommender algorithms is user behavioral data collected through surveillance, not explicit user feedback. *See* Narayanan, *supra*, at 18. This data can include likes, clicks, comments, time spent watching, time spent lingering, and other indications that a piece of content held a user's attention. *Id.* at 18–19; *e.g.*, Meta Decl. ¶ 12. The algorithms use this data to construct profiles of users. Profiling a user enables a company to compare them to other users, showing them media that similar users engaged with heavily. Narayanan, *supra*, at 22. Any message—including contradictory ones—goes, so long as it maximizes the amount of time the user spends on the site.

Recognizing the distinction between content moderation and engagement maximization, the majority in *Moody* set aside the question of whether "feeds whose algorithms respond solely to how users act online—giving them the content they appear to want, without any regard to independent content standards" are expressive. *Moody*, 144 S. Ct. at 2404 n.5. Justice Barrett, who formed a swing vote for the majority opinion, wrote in her concurrence, "The First Amendment implications . . . might be different" for "a platform's algorithm [that] just presents automatically to each user whatever the algorithm thinks the user will like—e.g., content similar to posts with which the user previously engaged." *Id.* at 2410 (Barrett, J., concurring). And in his concurrence, Justice Alito contrasted newspaper editors' expressive curation from algorithms that "prioritize content based on factors that the platforms have not revealed and may not even know." *Id.* at 2438 (Alito, J., concurring in the judgement).

The fact that engagement-maximizing algorithms are inscrutable black boxes whose outputs are determined by machine learning and not human value judgements undermines their expressiveness. Four justices explicitly recognized that the extent to which curation is mediated by black-box algorithms impacts the First Amendment analysis, even when those algorithms are performing content moderation. Justice Barrett wrote in her concurrence that "technology may attenuate the connection between content-moderation actions (e.g., removing posts) and human

[6] https://neely.usc.edu/2024/12/10/algorithms-contain-both-expressive-and-functional-components/.

beings' constitutionally protected right" of expression. *Id.* at 2410 (Barrett, J., concurring). She noted that "If the AI relies on large language models to determine what is 'hateful' and should be removed, has a human being with First Amendment rights made an inherently expressive 'choice . . . not to propound a particular point of view'?" *Id*. Justice Alito added, "[W]hen AI algorithms make a decision, even the researchers and programmers creating them don't really understand why the models they have built make the decisions they make. Are such decisions equally expressive as the decisions made by humans?" *Id.* at 2439 (Alito, J., concurring in the judgement) (quotation marks and citations omitted). If using algorithms can attenuate the expressiveness of otherwise-expressive *content moderation*, the case for the expressiveness of value-agnostic algorithmic *engagement maximization* is even more dire. If NetChoice wishes to argue that certain companies' engagement maximizing algorithms produce protected speech, they must reveal how those algorithms work and explain how they are expressive.

As it stands, there is nothing to suggest that engagement-maximizing algorithms, on their own, express any message of a company. They do not choose or rank content based on agreement or disagreement with the message expressed, only based on a user's likelihood of interacting with the media. Perhaps the most damning evidence against the expressiveness of engagement maximization is that platforms' recommendation algorithms often promote content that violates the company's guidelines or otherwise undermine their express priorities. *See, e.g.,* Sam Schechner et al., *How Facebook Hobbled Mark Zuckerberg's Bid to Get America Vaccinated*, Wall St. J. (Sep. 17, 2021);[7] Keach Hagey & Jeff Horwitz, *Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead*, Wall St. J. (Sep. 15, 2021).[8] How can the recommendation algorithm's amplification of messages the company says it disagrees with be expressive? This conflict exists precisely because the algorithms choose media for display without regard for the underlying message expressed.

SB 976 only regulates companies' use of engagement-based profiling in their content curation processes, not its content moderation practices. A feed is only addictive if it uses

[7] https://www.wsj.com/articles/facebook-mark-zuckerberg-vaccinated-11631880296.
[8] https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215.

certain personal information about a user, like behavioral data, to decide how content in the user's feed is arranged. Cal. Health & Safety Code § 27000.5(a). Regulating the use of personal data in the feed has no impact on companies' ability to prioritize, deprioritize, or block content that violates their policies. Because the Act only regulates non-expressive platform functions, and not expressive content moderation activities, it does not implicate covered entities' First Amendment rights.

The Act also leaves companies with ample room to organize and personalize users' feeds, despite NetChoice and its declarants repeated assertions otherwise. *See* Mot. at 13, 21 ("the Act restricts users' access to all personalized feeds"); Davis Del. ¶ 58; Vitech Decl. ¶ 40; Cleland Decl. ¶ 10. The Act explicitly allows companies to provide users with personalized feeds that reflect the users' own decisions about what authors, creators, and posters to follow. § 27000.5(a)(4). This type of personalization was the prevailing model of feed design until just a few years ago. *See* Narayanan, *supra*, at 9, 40 (showing that major companies moved toward algorithmic content selection and sorting between 2016 and 2022). The Act also does not prohibit companies from organizing feeds based on their value judgements or on the quality of content. Companies could provide curations of the best cat videos, or trending content, or breaking news. Instead of organizing this content based on timeliness, i.e., in reverse chronological order, companies can order content based on media-specific metrics like popularity, virality, and controversiality because these metrics are based on aggregate data and not necessarily information "persistently associated with the user" and "concern[ing] the user's previous interactions with media." § 27000.5 (a)(1). They could provide users with multiple feed options that they can toggle between, which many covered entities already do, like X's "Following" and "For you." Companies can also allow users to combine the companies' and other posters' curations into personalized feeds. *See* § 27000.5(a)(4) (wherein the company would be considered a "poster"). In short, the "addictive" aspect of addictive feeds is just not necessary for companies to organize or personalize content on their platforms.

II. NetChoice has not shown that the age assurance provision is likely to chill speech.

Moody's holding applies with equal force to NetChoice's challenge of SB 976's age assurance provision. It is not enough for NetChoice to rely on decades-old factual findings, to analogize SB 976 to very different laws, or to make assumptions about how companies will implement SB 976. NetChoice must instead develop a factual record specific to SB 976's age assurance provision, which NetChoice cannot do until the Attorney General has published his regulations. NetChoice's challenge to SB 976's age assurance provision is thus premature.

A. Reno and Ashcroft do not decide this case but do stress the importance of a timely and well-developed factual record on age assurance.

Reno v. ACLU, 521 U.S. 844 (1997) and *Ashcroft v. ACLU*, 542 U.S. 656 (2004) did not announce a categorical rule that age assurance is unconstitutional. The Court's First Amendment analyses in those cases relied heavily on extensive factual findings about the state of age assurance technology at the time they were litigated. Age assurance technologies—and the internet itself—have changed dramatically since *Reno* and *Ashcroft* were decided. NetChoice cannot rely on decades-old factual findings from these cases—it must build a factual record that reflects the current state of technology.

Reno only tangentially analyzed the constitutionality of age verification, and the Court relied on the trial court's extensive factual findings in its analysis. *Reno*'s central holding was that the Communications Decency Act ("CDA"), which broadly criminalized all transmissions of obscene or indecent materials to kids, was an unconstitutional content-based restriction on speech. *Reno,* 521 U.S. at 859–60. The *Reno* Court briefly addressed age verification because the CDA provided a defense for websites that used "effective" age verification tools to distinguish between kids and adults, but, following a trial on the merits, the district court found that there was no effective method in existence to prevent minors from accessing the proscribed communications without also denying access to adults. *Id.* at 876. The district court also found that there was no effective way to determine the age of users accessing materials in emails, listservs, newsgroups, and chat rooms. *Id.* Further, as a practical matter, the age assurance mechanism created a huge technological and financial burden that few websites could bear. *Id.*

at 877. For these reasons, few if any websites would actually implement age assurance, let alone in a way that would protect them in case of a lawsuit, and so the affirmative defense was "illusory" and could not save the CDA. *Id.* at 881.

The *Ashcroft* Court relied on extensive factual findings made by the district court and also insisted that the lower court update their findings on remand. *Ashcroft*, 542 U.S. at 672. The district court in the case had found that strict scrutiny should apply to the Child Online Protection Act's age verification requirement because, at the time, "the implementation of credit card or adult verification screens in front of material that is harmful to minors may deter [adult] users from accessing such materials." *ACLU v. Reno*, 31 F. Supp. 2d 473, 495 (E.D. Pa. 1999). The government did not dispute this finding on appeal. *Ashcroft*, 524 U.S. at 665. But the Court feared that technology had changed enough over the five years between the district court's fact-finding and the Supreme Court's review to render the district court's findings obsolete, and let the injunction stand on remand in part to allow the district court to engage in new factfinding. *Id.* at 671–72. The Court explained "the factual record [did] not reflect current technological reality—a serious flaw in any case involving the Internet." *Id.* The Third Circuit ultimately upheld the injunction based on the state of technology at the time. *ACLU v. Mukasey*, 534 F.3d 181, 196 (3d Cir. 2008).

If a five-year-old record was considered out of date at the time of *Ashcroft*, then the twenty-or-so year-old factual determinations relied upon in *Reno*, *Ashcroft*, and *Mukasey* are downright ancient. *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 20 (Sept. 30, 2024).[9] There is a much broader range of tools available to estimate age today than when those cases were decided, and SB 976 gives the Attorney General broad latitude to prescribe age assurance tools that don't verify age with certainty and that provide greater privacy protections than those available twenty years ago.

The internet of today is also very different than the internet at the time these cases were

[9] https://www.commonsensemedia.org/sites/default/files/featured-content/files/2024-us-age-assurance-white-paper_final.pdf.

litigated. Back then, surfing the internet was a largely anonymous endeavor. Today, people are surveilled as a matter of course when online, thanks in large part to companies in whose name NetChoice is challenging SB 976, like Google and Meta. These companies make their billions by tracking users' every interaction with their platforms, spying on them across the internet, and creating intricate profiles of users that could be used to identify them. *See* Electronic Privacy Information Center, Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem 36–38, 61–62 (2022).[10] Age assurance, backed by proper privacy protections, would be less invasive than the data practices these companies currently employ.

B. Unlike laws enjoined in other states, SB 976 does not require companies to verify users' ages, block kids from accessing platforms, or perform age assurance as a condition of access.

NetChoice relies heavily on decisions enjoining social media laws that bear little resemblance to SB 976. Those laws require companies to *verify* the ages of users, meaning that the companies need to have a very high certainty of a user's age before they can access the service. *See, e.g., 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*, No. CV 24-170-HSO (BWR), 2024 WL 3276409, at *1–*2 (S.D. Miss. July 1, 2024), *appeal docketed*, No. 24-60341 (5th Cir. July 5, 2024); *NetChoice, LLC v. Yost*, 716 F. Supp. 3d 539, 547 (S.D. Ohio 2024); *NetChoice, LLC v. Griffin*, No. CV 23-05105, 2023 WL 5660155, at *1, *3 (W.D. Ark. Aug. 31, 2023). SB 976 involves "age assurance," a much broader category of age determination techniques that estimate age to varying levels of certainty. Fox Johnson, *supra*, at 5–11. Techniques that estimate age to a lower level of certainty often do not require the same level of data collection and processing as age verification techniques, and so they do not present the same privacy, security, or access risks.

Many of the cases NetChoice relies upon also involve laws that block minors from accessing entire social media platforms, and thus implicate minors' First Amendment right to

[10] https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf.

access content on those platforms. *E.g., Fitch*, 2024 WL 3276409, at *1-*2; *Yost*, 716 F. Supp. 3d at 546; *Griffin*, 2023 WL 5660155, at *1. SB 976 does not require companies to bar minors from accessing their platforms: it only requires companies to turn off or limit certain harmful features. § 27000.5(a). Because these features are not protected speech, preventing minors from accessing them without parental consent does not impact minors' First Amendment rights. Minors are still able to access all content on regulated platforms as well as on any feed that doesn't surveil and profile them.

SB 976 also does not require companies to force users to go through the age assurance process *before* accessing the company's platform. § 27001(a). Instead, under SB 976, companies could make the rules for minors the default for all users and only estimate a user's age if the user wants to change one of these default settings. In other words, covered entities can age gate the regulated *features* and not their *platforms*. Companies could, e.g., turn addictive feeds off for all users by default and only require users who wish to turn these features on to go through the age assurance process. Assuming the age assurance tool a company uses actually does impede users' access to the gated feature, the impact would only be to impede users' access to *addictive feeds*, not to the platform as a whole. *See id*. Since addictive feeds are not protected speech, implementing age assurance in this way would not have any impact on users' (or companies') First Amendment rights. Companies would be free to provide any other feed to users, regardless of age, and users would be free to access all content and non-addictive feeds on the platform, without the need to undergo age assurance.

C. NetChoice's challenge to the age assurance provision is premature and NetChoice has otherwise failed to build an adequate record.

Determining whether age assurance is likely to deter users from accessing protected speech is a fact-intensive inquiry that must be supported by a robust factual record. Different age assurance tools carry different privacy risks. Any deterrent effect of age assurance will also vary from covered entity to covered entity, depending on their implementation strategy and their current data and design practices. *See* Sarah Forland, Nat Meysenburg & Erika Solis, *Age Verification: The Complicated Effort to Protect Youth Online,* New America Foundation Open

Technology Institute 11-12 (2024).[11] Consequently, in evaluating a sweeping challenge like NetChoice's, the court must consider, for each specific age assurance tool allowed under the law, and each regulated entity, the privacy risks and access burdens posed by the specific tool the company plans to use, how the law mitigates or enhances these risks, and whether use of the tool on the company's platform is actually likely to chill users' speech.

This Court cannot decide whether SB 976's age assurance provision chills access to speech because NetChoice has not assembled the record necessary to evaluate its claims. Indeed, it will be impossible for NetChoice to assemble such a record until after the Attorney General promulgates rules to implement the Act's age assurance requirement. Until then, it is not clear which age assurance tools are permissible under SB 976. Because age assurance technology is rapidly evolving, it is possible that the tools the Attorney General approves have not been released yet. It is also not clear how the Attorney General will use regulations to address potential privacy, security, access, and disparate impact concerns.

To properly evaluate the impact of SB 976's age assurance provision, the parties need to establish the full range of age assurance tools companies may use to comply with the law. Not all age assurance tools pose the same privacy and security risks to users. *Id*. The risks will depend on the specific technique used to estimate age and the data practices of the companies involved in the age assurance process. *See* Noah Apthorpe, Brett Frischmann & Yan Shvartzsnaider, *Online Age Gating: An Interdisciplinary Investigation* 16–20 (Aug. 1, 2024).[12] Some techniques involve higher risks because they involve collecting sensitive personal information, like driver's licenses or credit cards. But some techniques may only require users to provide a photograph or their email address, which users routinely provide to entities regulated by SB 976. How a tool actually works is important, and broad analogies are not helpful. For example, biometric age estimation should not be conflated with biometric identification. Biometric age estimation tools do not generally create biometric identifiers of

[11] https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/.

[12] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4937328.

users and so carry much lower privacy risks than facial recognition technology used to identify people. *Id*. at 21–22.

The data practices of the company providing the age assurance tool (if it is a third-party vendor) and the data practices of the covered entity can also increase or decrease privacy and data security risks. Companies that practice data minimization—collecting, processing, and retaining the minimum amount of information necessary to estimate whether a user is a minor—are more privacy protective than those companies that collect more than necessary. Tools that process and store users' personal information on users' devices or in their browsers are also more privacy-protective than tools that process and store information on the company's remote servers. *See* Fox Johnson, *supra*, at 10. Tools that transmit age determinations with privacy-protective technology like zero-knowledge proofs minimize risks to users, while tools that transmit users' identifying information in a way that allows them to be linked to their internet activities increase risks. Apthorpe et al., *supra*, at 22–25.

Similarly, not all age assurance tools will create the same barriers to use, what technologists refer to as "friction." *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). The difficulty of using an age assurance tool is likely to vary from user to user, and companies can mitigate the burden by providing users with a menu of options for age assurance. But some tools would be nearly frictionless because they would be run in the background. For example, some companies are likely already able to estimate the age of users using existing data. Companies like Meta and Google, whose platforms have been in existence for many years, could use account age as a first pass on estimating users' ages. Someone who joined Gmail or Facebook before 2010 is highly unlikely to be a minor. Additionally, companies that estimate the age of users to serve them ads should be able to use those estimates to comply with SB 976. *See* Nico Grant et al., *YouTube Ads May Have Led to Online Tracking of Children, Research Says*, N.Y. Times (Aug. 17, 2023).[13] Meta is also developing ways to proactively identify

[13] https://www.nytimes.com/2023/08/17/technology/youtube-google-children-privacy.html.

accounts that belong to teens that would run in the background and thus be invisible to users. *See* Meta, *Introducing Instagram Teen Accounts: Built-In Protections for Teens, Peace of Mind for Parents* (Sep. 17, 2024);[14] *see also* Davis Decl. ¶ 36. Users flagged by this process would be labeled as teens and given the option to verify their age to switch to an adult account. The Attorney General could encourage other companies to develop similar procedures, using low- or no-friction methods to label users as likely minors or likely not minors and require affirmative age assurance only when an account is flagged as likely belonging to a minor.

Protections provided by law can also mitigate the privacy, security, and access burdens from age assurance. SB 976's requirements that companies delete the personal information used for age assurance immediately and not use the data for other purposes greatly reduce the privacy and security risks to users. § 27001(b). If covered entities comply with the law, sensitive personal information like people's driver's licenses, credit cards, and other identifying information would not be at risk of theft because they would only be used to determine whether the user is a minor and then immediately deleted. Californians are also protected by the California Consumer Privacy Act. Cal. Civ. Code § 1798.100.

The Attorney General can also regulate age assurance through rulemaking. *See* Cal. Health & Safety Code § 27006(b). The New York Attorney General has already begun rulemaking to implement a very similar law, NY SAFE for Kids Act, N.Y. Gen. Bus. Law §1501(2) (McKinney 2024), and the breadth of that rulemaking is instructive, N.Y. Off. of Att'y Gen., Advanced Notice of Proposed Rulemaking for the Stop Addictive Feeds Exploitation for Kids Act 4-7 (Aug. 1, 2024).[15] The Attorney General's regulations regarding age assurance can keep pace with emerging technology, build on the Act's privacy and security protections, prioritize tools and vendors that are more privacy protective, require companies to give users a menu of choices for age assurance, require routine disclosures about age assurance data practices, and require other trust-enhancing steps from companies. *See* Electronic Privacy Information Center, Comments to the New York State Attorney General on the Advance Notice

[14] https://about.fb.com/news/2024/09/instagram-teen-accounts/.
[15] https://ag.ny.gov/sites/default/files/2024-08/safe-forkidsact.pdf.

of Proposed Rulemaking for the SAFE for Kids Act 8–21 (Sept. 30, 2024).[16] SB 976 also explicitly requires the Attorney General to "solicit public comment regarding the impact that any regulation might have based on the nondiscrimination characteristics" set forth in state and federal law, which means that the Attorney General's regulations must consider potential disparate impacts on people of color, immigrants, people with disabilities, and the LBGTQ+ community. Cal. Health & Safety Code § 27006(c).

Finally, the privacy, security, and access burdens introduced by an age assurance tool cannot be evaluated in isolation. Instead, courts must consider the impact of each age assurance tool on each covered entity's platform. If a platform provides users with a truly anonymous browsing experience—no tracking, no profiling, no selling or disclosing of their data to third parties—and an age assurance tool would significantly deter users from accessing protected speech on the platform, then that tool may chill users' access to protected speech on that specific platform.[17] But if a website already requires users to sign in, to use their real names, or to provide payment or other personal information, the calculus would be different, because these websites already require users to jump through hoops or provide personal information to access services. The extent to which covered entities already provide age assurance or identity services is also telling—namely, that age assurance may not significantly deter user access. Indeed, some of the companies challenging SB 976 require users to *pay* for identity services, signaling that many users are more than willing to provide these companies with the information necessary to estimate their ages. Meta, *Meta Verified* (2024);[18] X, *About X Premium* (2024).[19]

Importantly, companies that track their users, assemble profiles about them, or sell or

---

[16] https://epic.org/wp-content/uploads/2024/10/EPIC-Comments_NY-SAFE-For-Kids-Act.pdf.
[17] Dreamwidth claims to be in this position. Paolucci Decl. ¶¶ 17–18. But it is not at all clear the company is a covered entity. The only feature of its website that its declarant thinks might qualify as an addictive feed very likely does not—it only uses information about the creators a user follows to construct the feed, precisely what Cal. Health & Safety Code § 27000.5(a)(4) allows. Paolucci Decl. ¶ 12. Even if this feed were an addictive feed, it does not appear to be a "significant part of the service," and so Dreamwidth is unlikely to be considered an "addictive internet-based service or application." Cal. Health & Safety Code § 27000.5(b)(1).
[18] https://about.meta.com/technologies/meta-verified.
[19] https://help.x.com/en/using-x/x-premium.

share their data with third parties for advertising or other purposes do not provide their users with anonymous experiences, and it is unclear that age assurance would deter users from using these platforms. To the extent that these companies fear that users would not trust them with their personal information for age assurance purposes, the companies should *change their own business practices* to increase user trust, and not use a problem they created to get out of common-sense regulation.

CONCLUSION

For the foregoing reasons, *Amicus* ask this Court to deny Plaintiff's request for a preliminary injunction.

Dated: December 10, 2024

Respectfully submitted,

By: */s/ Alan Butler*

Alan Butler (SBN 281291)
butler@epic.org
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Avenue NW
Washington, DC 20036
Tel: 202.483.1140

Attorney for Proposed Amicus Curiae Electronic Privacy Information Center