No. 23-1122

IN THE
Supreme Court of the United States

FREE SPEECH COALITION, ET AL.,
Petitioners,

v.

KEN PAXTON, IN HIS OFFICIAL CAPACITY AS ATTORNEY GENERAL FOR THE STATE OF TEXAS,
Respondent.

On Writ of Certiorari to the U.S. Court of Appeals for the Fifth Circuit

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER IN SUPPORT OF NEITHER PARTY

ALAN BUTLER
Counsel of Record
MEGAN IORIO
THOMAS MCBRIEN
SUZANNE BERNSTEIN
ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)
1519 New Hampshire Avenue NW
Washington, DC 20036
(202) 483-1140
butler@epic.org

September 23, 2024

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE *AMICUS CURIAE*

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues.[1]

EPIC regularly participates as *amicus* in this Court and other courts in cases concerning privacy rights, speech rights, and internet regulations. EPIC was one of the plaintiffs seeking to protect adults' access rights in both *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997) and *Ashcroft v. American Civil Liberties Union*, 542 U.S. 656 (2004). EPIC has submitted *amicus* briefs to the Supreme Court concerning the proper evaluation of First Amendment challenges to platform regulations. *See, e.g.,* Br. of EPIC as Amicus Curiae, *Moody v. NetChoice* and *NetChoice v. Paxton*, 603 U.S. ____ (2004). EPIC has also submitted amicus briefs in federal circuit and district court cases involving First Amendment challenges to privacy and platform transparency laws. *See, e.g.*, Br. of EPIC as Amicus Curiae, *X Corp. v. Bonta*, No. 24-271, 2024 WL 4033063 (9th Cir. Sep. 4, 2024); Br. of EPIC as Amicus Curiae, *NetChoice v. Bonta*, No. 23-2969, 2024 WL 3838423 (9th Cir. Aug. 23, 2024).

---

[1]In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

SUMMARY OF THE ARGUMENT

Online censorship is a real and pernicious threat to Americans' First Amendment rights. EPIC has fought against online censorship consistently over its thirty-year history, and even participated as a plaintiff in the Court's two seminal online censorship cases: *Reno v. ACLU*, 521 U.S. 844 (1997) and *Ashcroft v. ACLU*, 542 U.S. 656 (2004). We also recognize that tech companies' harmful and invasive business practices threaten the privacy and safety of Americans—particularly kids. We thus advocate for and support generally applicable commercial regulations aimed at protecting kids online. But we are concerned about an alarming trend of tech companies bringing sweeping First Amendment challenges against these laws. That is why it is important for the Court to take special care in this case to apply a constitutional framework capable of distinguishing unconstitutional censorship laws from constitutional kids' privacy and safety laws.

We agree with Petitioners that the Fifth Circuit erred in applying rational basis scrutiny to H.B. 1181 under *Ginsberg v. New York*, 390 U.S. 629 (1968). We also agree with Petitioners that, if H.B. 1181's age verification requirement does have a substantial chilling effect on adults' access to protected materials, strict scrutiny should apply. But a largely unexamined and critically important question in this case is whether the age verification provision in H.B. 1181 *actually would* chill adults' speech. The Court's precedent provides little guidance on how to evaluate the claim that age assurance—meaning age verification or estimation—chills adults' access to protected materials. The Court should provide this guidance now, especially as

there is a growing interest in enacting other laws that use age assurance to help protect kids online.

Whether H.B. 1181—or any other law requiring age assurance—is likely to chill adult access to such an extent as to trigger First Amendment scrutiny is a highly statute- and fact-specific inquiry. Facial challenges to laws involving age assurance must be based on more than mere speculation and must meet the demanding standard reiterated in the Court's recent decision in *Moody v. NetChoice, LLC*, 144 S. Ct. 2383 (2024). This means building a record detailing, with specificity, the different age assurance methods prescribed by the law, the burden these methods impose on users, and whether adults would be deterred from accessing each type of service covered by the law.

If the Court decides against Texas in this case, it should issue a narrow opinion that leaves open the possibility for states to pass and enforce kids' privacy and safe design laws that include age assurance provisions. There is a real danger that some litigants will use a decision against Texas in this case to argue that any privacy or platform design law that involves any age assurance method is categorically unconstitutional.

Online privacy and safety laws that involve age assurance vary greatly in constitutionally salient ways, and their constitutionality should be decided on a case-by-case, not categorical, basis. While laws like H.B. 1181 are content-based, others are content-neutral, requiring companies not to restrict kids' access to content but to give kids heightened privacy protections and protect them against harmful designs. The specifics of the age assurance provisions in these laws also vary widely, and some are more likely to chill adult

access than others. And age assurance technology is rapidly evolving; more accurate and privacy-protective age assurance methods may be on the horizon, which means courts must re-evaluate the technological context whenever a new law is challenged. A decision in this case should not prevent legislatures from enacting strong protections for kids online, as long as they do so in ways that respects kids' (and adults') privacy.

ARGUMENT

I. The nature of the constitutional challenge in this case is fundamentally different than in the Court's precedent.

The question presented in this case is one of first impression for the Court. The cases relied upon by the Respondent involved claims that the challenged regulations burdened kids' speech offline, not adult speech online. The cases relied upon by Petitioners indicate that the Court should apply strict scrutiny if H.B. 1181 is, in fact, likely to chill adults' access to First Amendment-protected materials. But they do not help decide whether H.B. 1181's age assurance[2] requirement *actually is* likely to chill speech. To the extent that these cases analyze the impact of online age assurance on adult access, they do so in ways that are not applicable to the present case. It is especially

[2] "Age assurance" is an umbrella term that refers to any system that in some way vets a user's age. *See* Sarah Forland, Nat Meysenburg & Erika Solis, New America Foundation Open Technology Institute, *Age Verification: The Complicated Effort to Protect Youth Online* 10 (2024). It encompasses both age *verification*, which conclusively determines a user's age, and age *estimation*, which infers or estimates age. *Id.*

improper for courts to rely on the factual records in these cases, which are over 20 years old. The Court has previously remarked that it is "a serious flaw in any case involving the Internet" to issue a constitutional determination on the basis of a "factual record [that does] not reflect current technological reality." *Ashcroft v. ACLU*, 542 U.S. 656, 671 (2004). The Court should not mechanically apply distinguishable precedent in this case and instead should demand that the lower courts base their decisions on a robust record reflecting the current state of technology.

A. Laws that involve age assurance may burden kids' and adults' speech in different ways and require different threshold analyses.

Laws that involve covered entities either estimating or verifying the ages of users have a unique structure, and this structure impacts the nature of potential constitutional challenges. The nature of the constitutional challenge in turn dictates how courts should analyze whether and to what extent the law implicates the First Amendment. A challenge alleging burdens to kids' speech may only require determining whether the statute is a valid content-based restriction on speech for kids. But if the claim is that the law burdens adults' speech, the threshold inquiry must also involve an analysis of whether the age assurance mechanism actually does burden adults' access to protected materials.

Laws that involve age assurance have two significant parts: a governance rule, which is the rule covered entities are directed to apply to users assigned to a certain age group; and an age assurance mechanism, which prescribes how covered entities are to determine

which age group users belong to. *See* Noah Apthorpe, Brett Frischmann & Yan Shvartzsnaider, *Online Age Gating: An Interdisciplinary Investigation* 3 (Aug. 1, 2024).[3]

To the extent that laws involving age assurance burden speech, they will burden speech for kids and adults in different ways. A statute with a governance rule that says "kids can't access certain materials" may unconstitutionally burden kids' speech if kids have a constitutional right to access some of the restricted materials. But a governance rule that says "kids can't access certain materials" does not, on its face, burden adults' speech. Adults are inherently exempt from the governance rule. It is only through the governance rule's interaction with the age assurance mechanism that adults' speech may be impacted. For instance, if the age assurance methods prescribed by the law are error-prone such that adults are often labeled as kids, a content-based restriction on kids' access to content may also restrict adults' access. If adults are unwilling to subject themselves to the age assurance methods required by the law because the methods are overly burdensome or present unreasonable privacy risks, adults' access to protected materials may also be chilled.

Thus, when a litigant challenges the constitutionality of an age assurance law on its face based on the law's purported impact on adults, it is not enough for a court to decide whether the governance rule is content-based or content-neutral. Courts must also

---

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

determine, at the threshold, whether the age assurance mechanism actually burdens adults' speech.

B. The Court's offline age assurance cases involve challenges to kids', not adults', access and do not provide sufficient guidance to analyze claims that age assurance burdens adults' speech.

This Court has decided First Amendment challenges to *offline* age assurance statutes in the past, but these cases focused on claims that the statutes in question burdened kids' speech, not adults. As a result, the threshold inquiry in these cases was properly limited to whether the governance rule triggered First Amendment scrutiny. These cases did not consider whether offline age assurance mechanisms burden *adults'* access and so provide insufficient guidance on how to analyze challenges like the one in this case.

Take, for instance, *Ginsberg v. New York*, 390 U.S. 629 (1968). The statute at issue directed purveyors of materials considered obscene for kids to verify the ages of customers and to not sell such materials to kids. *Id.* at 645–47. The law's challenger was convicted of selling obscene materials to a minor, and, in an attempt to overturn that conviction, argued that the government could not criminalize the distribution of such materials *to minors*. *Id.* at 636. The challenge was thus premised on the statute's burden to *kids'* speech, and that burden was entirely traceable to the law's governance rule—"do not sell obscenity to minors." *See id.* at 636–37. The Court thus appropriately limited its First Amendment analysis to the governance rule and found that rational basis scrutiny applied because kids do not have a constitutionally protected interest in accessing the regulated obscenity. *Id.* at 637.

Consider also *Brown v. Entertainment Merchants Association*, 564 U.S. 786 (2011), which concerned a law restricting the sale of violent video games to minors. Here, too, the law's challengers claimed that the governance rule—"don't sell violent video games to minors"—violated *kids'* protected speech. *Id.* at 794–96. The Court thus needed to look no further than the governance rule to find that strict scrutiny applied because kids *do* have a constitutionally protected interest in accessing video games and the law imposed a content-based restriction on such access. *Id.* at 799.

Both *Ginsberg* and *Brown* were silent on the First Amendment implications of in-person age verification because the statutes' age assurance mechanisms were irrelevant to the constitutional challenges at issue, not because in-person age verification only triggers rational basis scrutiny, as the Fifth Circuit panel majority inferred. *See* Pet. App. 10a. And while it may well be the case that offline age assurance does only trigger rational basis scrutiny, *Ginsberg* does not explain why. *Ginsberg* accordingly does not provide guidance on how to evaluate a claim that age assurance chills adult access offline, let alone online. Lower courts need guidance from this Court as to what factors to consider in deciding whether an online age assurance mechanism imposes an undue burden on adult access.

C. The Court's cases about adult censorship either were not premised on age assurance's chilling effect on adult access or assumed but did not decide that age verification chilled adult access.

The suite of Supreme Court cases Petitioners rely upon involved challenges to statutes that sought to restrict kids' access to adult materials and, in the process, also restricted adults' access. Only one of these cases involved a claim that the law's online age assurance mechanism chilled adult access to protected materials, but even that case did not analyze the threshold question of whether and to what extent there was an actual chill. These cases, at most, say to apply strict scrutiny to H.B. 1181 if it does, in fact, chill adults' access to protected materials. But they do not provide sufficient guidance about what factors courts should consider in evaluating, at the threshold, whether a statute's age assurance mechanism *actually does* chill adults' access.

The laws at issue in both *Sable* and *Playboy* created across-the-board prohibitions on speech and so imposed direct restrictions on adults' access to speech. In *Sable*, all persons—kids and adults—were unable to access dial-a-porn services. *Sable Commc'ns of California, Inc. v. FCC*, 492 U.S. 115, 123 (1989). And in *Playboy*, all persons—kids and adults—were unable to access Playboy broadcasts from 6 a.m. till 10 p.m. *United States v. Playboy Ent. Grp., Inc.*, 529 U.S. 803, 808 (2000). Because neither case involved a law with an age assurance mechanism, neither case provides guidance on how to evaluate a claim that age assurance chills adults' access to protected materials.

The constitutional challenge in *Reno v. ACLU* was much more similar to the challenges in *Sable* and *Playboy* than to the challenge in the present case. *See Reno v. ACLU*, 521 U.S. 844, 875 (1997) ("The District Court was correct to conclude that the CDA effectively resembles the ban on "dial-a-porn" invalidated in *Sable*."). The *Reno* Court applied strict scrutiny to the Communications Decency Act ("CDA") because the law's vague, overbroad governance rule would burden both kids' and adults' access to protected materials, not because the law's age assurance provision burdened speech. *Id*. at 879.

The CDA criminalized the act of transmitting obscene or indecent materials to kids. *Id.* at 859–60. The Court found that this would burden both kids' and adults' right to access constitutionally protected materials. It burdened kids' rights because its definition of the prohibited materials lacked the constitutionally required narrowing provisions that other kids' protection laws had, such as exceptions for materials with redeeming social importance. *Id*. at 873–74. And it burdened adults' rights by failing to properly inform them of the scope of the prohibited materials. Adults would not know whether a given discussion topic was criminal because different sections of the law used different definitions for the prohibited materials, and these definitions used vague terms such as "indecent." *Id*. at 870–71. This lack of guidance about which topics could land one in prison would likely cause adults to engage in self-censorship and online intermediaries to censor sensitive conversations. *Id.* at 872. The *Reno* Court's decision to apply strict scrutiny has limited applicability to other laws that do not criminalize speech based on content and that are not vaguely drafted.

The *Reno* Court briefly addressed age assurance because the CDA provided a defense for websites that used an age assurance mechanism to distinguish between kids and adults.[4] The government argued that this defense would preclude any overbreadth concerns: if companies excluded kids from adult-only conversations, then adults would have no need to self-censor, and online intermediaries would have no need to censor adult conversations. *Id.* at 881–82. But the CDA required companies to use "effective" age verification methods to invoke the defense, and, 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 noncommercial—and some commercial—websites could not bear. *Id.* at 877. The affirmative defense was thus "illusory." *Id.* at 881. 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. Adults would be governed by the censorship rule to the same extent as kids.

---

[4] The affirmative defense applied to websites that took "good faith, reasonable, effective, and appropriate actions" to restrict minors' access to prohibited communications or "restricted access to such communications by requiring use of a verified credit card, debit card, adult access code, or adult personal identification number." *Reno*, 521 U.S. at 860–61.

In *Ashcroft*, the Court did not examine whether the Child Online Protection Act's age assurance provision triggered strict scrutiny, *Ashcroft v. ACLU*, 542 U.S. 656, 665 (2004), but it did insist upon having specific, up-to-date facts about age assurance when evaluating its constitutionality. *Id.* at 672. The district court in the case found that strict scrutiny should apply 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). Because the government did not dispute this finding on appeal, the threshold issue of whether strict scrutiny applied was not up for review. *Ashcroft*, 524 U.S. at 665. For this reason, the opinion provides little guidance on how courts should evaluate age assurance's burden on speech.

What the *Ashcroft* Court did do was to insist on courts' having specific, timely facts about internet technology when evaluating how that technology might impact speech. The Court decided to let the injunction in *Ashcroft* stand on remand in part to allow the district court to engage in new factfinding. *Id.* at 671. It feared that technology had changed enough over the five years between the district court's factfinding and the Supreme Court's review to render the district court's findings obsolete. *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 *Ashcroft* Court would presumably disapprove of its holding being mechanically applied to an age assurance law passed 20 years after it issued its opinion. The Court in this case, and any other case involving the constitutionality of

internet technologies, needs an up-to-date and factually specific record.

II. Whether and to what extent an age assurance mechanism chills adults' speech depends on the specific requirements of the law and the technical, legal, and social context at the time of the challenge.

This Court recently reiterated the high standards that plaintiffs need to meet in a facial First Amendment challenge. The decision to bring a facial instead of an as-applied challenge "comes at a cost." *Moody v. NetChoice, LLC*, 144 S. Ct. 2383, 2397 (2024). That cost is the time and attention it takes to construct a detailed, specific record that enables a reviewing court to ensure its decision is not based on speculation and does not short-circuit the democratic process by preventing the constitutional application of duly enacted laws. *See id.* at 2397–98. In this case, the record should include detailed and specific facts about the full range of age assurance methods required or permitted under the law and relevant facts about the regulated websites so that a court can determine which of the law's applications will likely burden users' access rights and which will not.

A. In a facial challenge, courts must be able to determine the full scope of age assurance methods authorized under the law and make findings about how each option would actually be implemented.

It is impossible for a court to determine whether and to what extent an age assurance law chills adult access without first establishing what age assurance methods are required or permitted under the law and

how available tools actually work. Age assurance methods vary widely, and specific facts about who is providing the service, how they verify or estimate a user's age, and how they manage data are all relevant to whether adults' speech is likely to be chilled. In a facial challenge, particularly one brought by the covered entities who have a choice as to which age assurance method to use, courts must determine the full scope of age assurance options because some may deter adult users while others may not. The availability of age assurance options that do not burden adult access undermines a covered entity's claim that the law burdens adults' speech.

First, courts need to be able to identify the range of age assurance methods that can be used to comply with the law. A law can mandate that covered entities use a specific assurance method, allow them to choose from a set range of methods, or provide a flexible standard that allows different websites to implement different methods depending on their specific circumstances.[5] The types of age assurance methods prescribed in laws can vary widely, including:

- Providing a government ID
- Providing proof of credit card ownership
- Biometric scan of a face or voice
- Age estimation using existing company data

---

[5] For instance, the California Age-Appropriate Design Code directs covered entities 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," Cal. Civ. Code § 1798.99.31(a)(5), and to ensure that "age assurance [] be proportionate to the risks and data practice" of the company, *id.* at (b)(8).

- Parental attestation
- Self-attestation

See Forland et al., *supra* note 2, at 10–18. Different methods carry different privacy risks. The ultimate determination on whether they are likely to burden speech will be highly fact-based.

Once a court determines which categories of age assurance methods can be used to comply with the law, it then needs to make findings about how those methods can be implemented. Most companies are likely to contract with a third-party vendor for an age assurance tool, so the court should make findings about specific available vendors, how their tools work, and what their data practices are. *See id.* They should also make findings about what information the third-party tools communicate to the service the user is trying to access, and vice-versa. All of these factors together help determine what kinds of personal information the covered entities and third-party age assurance vendors will be allowed or required to collect and, in turn, help determine what privacy risks users might face. *See* Mohammed Raiz Shaffique et al., European Commission, *Research Report: Mapping Age Assurance Typologies and Requirements* 33–34 (2024).

How the available age assurance tools work also matters because there can be key differences between tools even within the same general category of age assurance method. For example, some tools may process users' personal information on-device or in their browser, while others may process the data remotely on the vendors' servers. Scott Babwah Brennan & Matt Perault, *Keeping Kids Safe Online: How Should Policymakers Approach Age Verification?* 4 (2023). Tools that process data on users' devices do not expose

users to the same privacy and security risks as tools that process on the vendors' servers. Some tools may also allow a user to verify their age once and then issue them a virtual credential that essentially says "I am over X age" that they can use to enter age gates on other services without the need to re-verify their age. Some tools may use "zero-knowledge proofs" to confirm a user is displaying a valid credential without allowing the website to learn any additional information about the user, like their identity, and without allowing the age assurance vendor to learn any additional information, such as the websites the user visits. *See* Forland et al., *supra* note 2, at 12.

Laws that require the government to either perform the age assurance, issue special identification credentials, or maintain any records about access carry special risks of enabling government surveillance. But, contrary to what the district court in this case seemed to assume, the government need not be involved in verifying users' ages through government ID. Many third-party vendors perform this service, not by transmitting information to the government, but by extracting the date of birth from the government ID and then comparing the photo on the ID to a selfie that the user provides in real-time. *See id.*

The district court's confusion about who would perform government ID age verification seems to stem from the lack of development of a factual record in this case. Indeed, the district court made startlingly few factual or legal findings about how age assurance would actually be implemented in response to H.B. 1181. *See* Pet. App. 107a–111a. The clearest findings were on what age assurance methods H.B. 1181 would *not* allow—vouching and biometric assessment—but

not about the methods it *would* allow. *See id.* at 129a. The Fifth Circuit panel majority also contradicted the district court's finding that biometric age estimation was not allowed under the law without making any finding of error, which adds additional confusion to the record. *Id.* at 11a.

B. Courts must analyze the privacy and user trust implications of laws with specificity.

Once the court has a record evaluating the range of the law's potential applications, it can assess each application's likely impact on speech. The district court was correct that user trust in companies' privacy practices impacts users' willingness to provide third parties with personal information. But both the District Court's and the Fifth Circuit's analyses of H.B. 1181's impact on user trust and privacy were cursory. The privacy risks posed by age assurance tools should be analyzed with specificity. So should the privacy protections afforded by both technology and the law, as these can enhance user trust. Covered entities can also influence user trust by choosing more privacy-protective age assurance methods, using more trustworthy vendors, integrating tools that allow for user choice and interoperability between platforms, informing users of their rights and the websites' responsibilities, and generally by adopting more privacy-protective practices.

Given the current state of technology, it may very well be the case that every available age assurance method that H.B. 1181 allows imposes privacy risks on users that will deter them from accessing the regulated content. But the district court did not specifically analyze the privacy implications of each available method. Neither did the Fifth Circuit panel

majority, which essentially assumed not only that biometric assessment was an allowed method of age assurance (in contradiction to the district court), but also assumed without any analysis that available methods imposed no more privacy risks on users than in-person age verification. Pet. App. 11a. Using the proper framework matters, even if it does not change the answer in this case, because it might change the answer in *another* case.

The operative question when evaluating the privacy risks of an age assurance mechanism is not whether there are *any* privacy risks but whether those risks are substantial enough that users are likely to be deterred from accessing protected materials. Offline age assurance, for instance, involves some privacy risks. Customers are typically required to hand over a government ID that lists their full name and home address. In the pornography context, clerks can spread gossip about customers in their communities, causing acute embarrassment. Some customers may even be deterred from purchasing such materials in stores because they have a public profile, or because they know the clerk. Yet, to *Amicus'* knowledge, there has never been a serious First Amendment challenge to in-person age verification, and courts and litigants often use in-person age verification as a baseline to measure the potential chilling effect of online age assurance. There is thus, at the very least, a social acknowledgement that some burden on adult access is acceptable.

The user information an online tool collects, processes, and stores generally defines its privacy risks. The more sensitive personal information a company collects, the higher the risk to users' privacy, and the more likely users are to think twice about providing

the information. The potential for a user's identity to be linked to their internet activity—particularly when that activity may involve accessing sensitive or controversial information—is a key factor in evaluating the privacy risk from age assurance. *See* Apthorpe et al., *supra*, at 19, 21.

Whether and to what extent linkability is a risk with a specific age assurance tool depends on the age assurance company's data practices. Age assurance tools can minimize privacy risks—and enhance user trust—by minimizing the amount of data they collect, process, store, and disclose. The most privacy-protective tools will not collect any identifying information at all. But tools that do collect identifying information can partially mitigate their privacy risks by deleting that information after verifying or estimating a user's age. Tools that use cryptographic techniques to communicate whether a user is an adult or a kid to the website they seek to access without providing the website with any additional information about the user—a "zero knowledge proof"—also minimize privacy risks and enhance user trust by ensuring that neither the website nor the age assurance vendor can link the users' identity to their internet activity. *See* Apthorpe et al., *supra*, at 23–26; Bandio, *Learn More* (2024).[6]

Covered entities can also play a role in enhancing users' trust. Users' reluctance to provide personal information to tech companies, and their lack of trust in companies' data privacy and security practices, does not stem from age assurance alone but also from background market and regulatory forces: tech companies' relentless pursuit of surveillance capitalism and

[6] https://www.bandio.com/learn-more-bandio.

legislatures' failure to regulate this conduct. *See* Apthorpe et al., *supra*, at 18. Companies should not be able to engage in monetization strategies that put users' privacy at risk and then turn around and use that fact to escape regulation. Companies should be expected to do their part to enhance user trust by improving their own privacy and security practices and informing users of the protections they, their contractors, and the law provide users.

A law involving age assurance can also mitigate the privacy risks posed by covered entities' or age assurance vendors' data management practices by providing users with enhanced privacy protections. Because tech companies have a market incentive to collect as much user data as possible, legislatures must include strong privacy protections in statutes that mandate data collection. Such privacy provisions can require covered entities and age assurance vendors to practice data minimization by only collecting, processing, and disclosing the personal information strictly necessary to determine whether a user belongs to a certain age group. The statute can also prohibit the use of personal information for any purpose other than age assurance, prohibit the transfer of personal information to additional third parties, prohibit government access absent a warrant, and mandate the immediate deletion of personal information used to make the age determination. *See, e.g.*, NY SAFE for Kids Act, N.Y. Gen. Bus. Law §1501(3) (McKinney 2024). Comprehensive privacy laws at either the state or federal level can also provide users with additional protections. But strong transparency and enforcement mechanisms are necessary to ensure that the legal protections are not merely illusory.

C. Courts must analyze the user experience implications of laws with specificity.

Courts should also review whether a law could chill users' access rights by imposing onerous age assurance processes on users. Users might decide not to access materials if they are unwilling to complete the steps necessary to assure their age. Design literature refers to this burden 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 friction burden is related to but distinct from the privacy burdens. For instance, an age assurance mechanism that estimates age by silently tracking users' behavior across the web may be frictionless, but it would present serious privacy concerns. Friction is a real but highly subjective factor that likely changes over time. Relevant factors to assess include the actual implementation of the age assurance methods provided by the law, the incentives facing covered services and age assurance vendors that impact how they are likely to incorporate age assurance, and evidence of users' opinions on different age assurance processes' levels of friction.

As with privacy risks, the operative question is not whether an age assurance tool adds any friction at all, but whether the friction would substantially burden speech. Many business regulations introduce friction into the customer transaction process. Laws that require companies to disclose information to customers before a purchase or that require customers to consent to certain business practices are examples. Offline age assurance often requires people to show government ID, which slows down the purchasing process.

Online privacy and safety laws also already impose friction on users. COPPA-covered websites often require users to complete self-attestation pop-ups, *see* Apthorpe et al., *supra*, at 20, and gambling and alcohol websites generally require users to enter their date of birth or provide other proof of age to access the website. *See* Beer Institute, *Advertising and Marketing Code* 5 (Sep. 2023) (alcohol industry self-regulatory guidelines requiring age assurance for websites); Lawful Internet Gaming Act, Mich. Comp. Laws § 432.307(c) (2019) (Michigan law requiring online gambling entities to verify age). Some major tech companies, like Google and Meta, already use age assurance techniques at issue in this case, like government ID and credit card checks, either voluntarily or to comply with laws in other countries. *See, e.g.*, Google, *Access Age-Restricted Content & Features* (2024)[7]; Meta, *Learn About ID Verification for Meta Accounts* (2024).[8] The ease with which users are able to pass through age assurance checks may well increase as more companies implement age assurance on their platforms.

To determine whether a given age assurance law is likely to introduce enough friction to substantially burden access rights, courts need sufficient facts to understand the likely effects of the challenged law. Age assurance tools vary in the friction they impose based on multiple factors, including:

---

[7] https://support.google.com/accounts/answer/10071085?hl=en.

[8] https://www.meta.com/help/quest/articles/accounts/privacy-information-and-settings/id-verification-meta-accounts/.

- **The number of steps a process requires users to take.** Each additional step can increase friction.
- **The difficulty of each step in the process**. For example, many users are already familiar with pop-ups, which could prompt a user to attest whether they are over 18 or test their knowledge on a trivia fact likely only known to adults. But requiring a user to find and produce a government ID may be more burdensome, especially for adult users who do not have them.
- **How often a user must undergo age assurance to access content.** Requiring a user to verify their age once is likely less burdensome than requiring users to assure age each time they visit a site or access restricted content. Third-party tools that allow users to verify once and use that credential to access multiple websites can drastically minimize friction.

These are just three of many potential considerations that courts need substantial records to gauge properly.

In evaluating the likely impact of friction on access, courts should also recognize that covered entities have a market incentive to make age assurance as easy as possible for users. *See* Digital Trust & Safety Partnership, *Age Assurance Guiding Principles and Best Practices* 13 (2023). The less friction an age assurance process creates, the more likely users are to use the service, and the more users who use the service, the more money the company makes. Companies

invest enormous amounts of time and money into designing their services to be as frictionless as possible, and there is little reason to expect differently when it comes to age assurance. Covered entities are thus likely to implement age assurance tools that keep the barriers to entry low and minimize the chill on access not just because users benefit but because *they* also benefit.

D. The baseline for measuring any chilling effect varies from website to website.

Facts about the online services covered by the law are also relevant in a facial challenge because the extent to which adults may be reluctant to submit to age assurance may vary from service to service. In a facial challenge, courts must determine the full scope of covered entities and decide how likely users are to be deterred from using the services if they must go through an age assurance process. *See Moody* 144 S. Ct. at 2398. They must then compare the unconstitutional applications to the constitutional ones. *Id.*

For example, anonymity is an important feature of many websites, but not all. Age assurance methods that force a user to identify themselves on a service where anonymity is an important feature may have a significant chilling effect. But if a website is only accessible through a subscription, users may already be required to provide the kind of information that can be used to verify their age, and so users may not be deterred from submitting to age assurance.

In the present case, covered entities include both subscription and non-subscription services. While users may be deterred from accessing the non-subscription websites if they are required to provide identifying information for access, it is far less clear that

users of the subscription services would be similarly deterred, since they already provide the companies with their credit card information for payment purposes. While the lower courts noted that both subscription and non-subscription services were covered by the law—and that both are among the Petitioners in this case—neither court recognized that this fact was relevant to the constitutional inquiry.

In sum, litigants need to develop detailed factual records in cases that seek to facially invalidate laws involving age assurance. This can be a tall order given the variety of age assurance methods available and the complex background factors that impact how users will respond to age assurance. But it is an important and legally required task to ensure courts can capably distinguish between unconstitutional restrictions on speech and constitutional, duly enacted privacy and safety laws. Because the current record in this case is not sufficiently developed, the Court should remand for further factual development in the district court.

III. The Court should leave open the possibility for legislatures to enact laws that give kids special protections online while also protecting their privacy.

There is growing public recognition that kids face serious privacy and safety risks online. *See* Kids Online Health and Safety Task Force, *Online Health and Safety for Children and Youth: Best Practices for Families and Guidance for Industry* 10 (2024). Tech companies face strong market incentives to capture kids' attention and data. These business practices run counter to kids' interests and can cause devastating harm. *Id.* at 17. To counteract the market incentives

tech companies face, and to minimize the risks to kids' safety and privacy online, legislatures have begun to enact laws that require companies to give kids special protections online. Tim Bernard, Stanford Program on Platform Regulation, *Legislative Approaches to Combating Online Harms to Children* 3 (2024). The Court should frame its decision in this case to preserve the ability for state and federal legislatures to continue to experiment with innovative, constitutional approaches to providing kids with special protections online, while also making clear when and why certain approaches to age gating the internet might violate the constitution.

A. Some content-neutral laws aimed at protecting the privacy and safety of kids online rely on age assurance.

Online age assurance laws are not monolithic. *Id*. at 8–18. Some laws, like the one at issue in this case, direct tech companies to block kids from accessing certain content or services. These laws also tend to require more invasive forms of age verification, in part to ensure that their content-based governance laws are accurately applied only to kids. But another set of kids' online protection laws direct companies to provide kids with higher privacy protections or shield them from manipulative design decisions. These privacy and safe design laws can help solve real and urgent problems that the public is increasingly recognizing require legislative solutions.

Age-appropriate design codes are one model for content-neutral kids' privacy and safety laws that have been implemented in two states: California and Maryland. *Id*. at 13–14. These laws do not direct companies to block kids from accessing content, but

instead require them to provide kids with additional privacy protections, including high privacy settings by default. Neither law requires companies to use age assurance—companies can choose to give all users heightened privacy protections—but for companies that do choose to use age assurance, the laws provide only a few limitations on the choice of method. The California Age-Appropriate Design Code ("CAADC"), for instance, requires companies choosing to implement age assurance 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." Cal. Civ. Code § 1798.99.31(a)(5). The law thus envisions companies using a broad range of age estimation techniques, like self-attestation, parent-attestation, and estimates based on existing data, that H.B. 1181 does not allow. Both the California and the Maryland design codes also require companies to adopt privacy-protective age assurance methods and to safeguard the data involved in the age assurance process. *See* Cal. Civ. Code §§ 1798.99.31(b)(3), (8); H.B. 603, 2023 Leg., 446th Sess. (Md. 2024) (to be codified at Md. Code Ann., Com. Law. §§ 14-4604, 14-4604(A)(8), (C) (West 2024)).

Other recently enacted and proposed laws would require companies to curb addictive design features like autoplay, autoscroll, push notifications, and algorithmic behavioral profiling. For example, New York recently enacted the SAFE for Kids Act, which prohibits companies from generating algorithmic feeds that respond primarily to how users act online unless the company has used "commercially reasonable and technically feasible" methods to determine that the user is not a kid or the user's parent has provided consent. NY SAFE for Kids Act, N.Y. Gen. Bus. Law

§1501(1) (McKinney 2024). The law also prohibits covered entities from sending kids push notifications at night. *Id*. §1502. The SAFE Act had an overwhelming amount of support from the public: 63% of New York voters responded in a poll that they supported the law. And the law passed the New York legislature without any opposing votes, even after Big Tech spent nearly a million dollars lobbying against it. Thomas Barrabi, *Meta, Google Leading Nearly $1M Lobbying Fight to Kill NY Online Child Safety Bills*, N.Y. Post (May 20, 2024).[9]

The outcome of the present case should not short circuit legislatures' efforts to enact these and other content-neutral laws involving age assurance. The framework the Court adopts in this case should be sensitive to the fact that there are a wide range of existing and potential online age assurance laws and that the differences between the laws have constitutional significance.

B. Lower courts need the aid of a narrow, detailed decision to address a flood of First Amendment challenges that elide the constitutionally salient differences among kids' online privacy and safety laws.

Privacy and design regulations that use age assurance to give kids special protections are fundamentally different than laws that block kids from accessing certain content or services. They are content-neutral, not content-based; and they also typically allow companies to implement less privacy-invasive and friction-

[9] https://nypost.com/2024/05/20/business/meta-google-leading-nearly-1m-lobbying-fight-to-kill-ny-online-child-safety-bills/.

causing age assurance tools than their content-based counterparts. But that has not stopped tech companies, most notably through their litigious trade group NetChoice, from conflating the two legislative approaches in First Amendment challenges to kids' privacy and safety laws. There is thus a real danger that tech companies will use a decision against Texas in this case to support their arguments that kids' privacy and safety laws are categorically unconstitutional, potentially closing the door on legislative approaches to ensuring kids safety online. A narrow and detailed explanation from this Court about the proper framework for determining the level of scrutiny to apply to H.B. 1181 will help lower courts properly evaluate challenges against other laws that involve age assurance in a way that preserves legislatures' ability to protect kids online.

There is ample evidence that tech companies are ready and willing to apply the Court's pronouncements broadly in an attempt to stymy regulation. One clear example is NetChoice's use of the *Reno* and *Ashcroft* decisions to attack content-neutral privacy and design laws that rely on age assurance. As discussed above, neither *Reno* nor *Ashcroft* squarely addressed the question of whether and when age assurance constitutes a burden on speech for content-based laws. *See supra*, Part I.C. Yet NetChoice claims that the cases ruled age assurance presumptively unconstitutional, even for *content-neutral* laws. *See, e.g.*, Pl's Reply Br., at *3, *NetChoice v. Fitch*, No. 1:24-cv-170-HSO-BWR, 2024 WL 3276409 (S.D. Miss. July 1, 2024) (citing *Ashcroft* 542 U.S. at 667; *Reno*, 521 U.S. at 881-82).

Upon obtaining an injunction against a content-based age assurance law in one jurisdiction, NetChoice

has then cited that order as support for challenges to other, very different kids' privacy and safety laws in other jurisdictions. For instance, in *NetChoice v. Griffin*, NetChoice obtained an injunction against a heavy-handed Arkansas law that prohibited any child from accessing social media without parental permission. *NetChoice, LLC v. Griffin*, No. 5:23-CV-05105, 2023 WL 5660155, at *2 (W.D. Ark. Aug. 31, 2023). It then cited *Griffin*, along with *Reno* and *Ashcroft*, in its suit to enjoin California's Age-Appropriate Design Code. *See* Pl.-Resp't's Res. Br., at *22–23, *25, *49–50, *NetChoice, LLC v. Bonta*, No. 23-2969, 2024 WL 3838423 (9th Cir. Aug. 16, 2024). The trade group has threatened the same treatment for New York's SAFE for Kids Act. *See* NetChoice, *NetChoice Condemns New York's New Unconstitutional Internet Censorship Law* (June 20, 2024).[10]

Kids online privacy and safety is an important and urgent goal. Legislatures are considering a variety of statutes aimed at protecting kids, some of which are likely constitutional and others not. The Court's decision in this case should guide lower courts to decide challenges to kids' privacy and safety laws on a case-by-case basis based on the current state of technology and specifics of the statutory structure, not on mechanical applications of precedent.

[10] https://netchoice.org/netchoice-condemns-new-yorks-new-unconstitutional-internet-censorship-law/.

CONCLUSION

For the above reasons, *amicus* EPIC respectfully asks this Court to vacate the judgment of the Court of Appeals for the Fifth Circuit and remand for further proceedings consistent with the Court's opinion.

Respectfully submitted,

ALAN BUTLER
MEGAN IORIO
THOMAS MCBRIEN
SUZANNE BERNSTEIN

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire
Avenue NW
Washington, DC 20036
(202) 483-1140
(202) 483-1248 (fax)
butler@epic.org

September 23, 2024