United States Court of Appeals

for the

Fifth Circuit

Case No. 25-51073

STUDENTS ENGAGED in Advancing Texas; M. F., by and through next friend VANESSA FERNANDEZ; Z. B., by and through next friend S.B.,

Plaintiffs-Appellees,

v.

KEN PAXTON, in his official capacity as the Texas Attorney General,

Defendant-Appellant.

consolidated with

Case No. 26-50001

COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION,

Plaintiff-Appellee,

v.

KEN PAXTON, in his official capacity as Attorney General of Texas,

Defendant-Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF TEXAS, AUSTIN, IN NOS. 1 :25-CV-1662 AND 1 :25-CV-1660, HONORABLE ROBERT L. PITMAN, U.S. DISTRICT JUDGE

BRIEF OF *AMICI CURIAE* BIPARTISAN TECHNOLOGY POLICY SCHOLARS IN SUPPORT OF DEFENDANT-APPELLANT AND REVERSAL

JOEL THAYER
Attorney for Amici Curiae Bipartisan Technology Policy Scholars
1255 Union Street NE, 7th Floor
Washington, D.C. 20002
(760) 668-0934

CP COUNSEL PRESS (800) 4-APPEAL • (393216)

CERTIFICATE OF INTERESTED PERSONS

The undersigned counsel of record certifies that the following listed persons and entities as described in the fourth sentence of Fifth Circuit Rule 28.2.1 have an interest in the outcome of this case. These representations are made in order that the judges of this Court may evaluate possible disqualification or recusal.

Students Engaged in Advancing Texas, *et al.*, Plaintiffs—Appellees

Ken Paxton, Defendant—Appellant

Joel Thayer and Professor Meg Leta Jones, *Amici Curiae*.

Joel Thayer is counsel for *Amici Curiae.*

Pursuant to Federal Rules of Appellate Procedure 26.1 and 29(c), and 5th Circuit Rule 28.2.1, it is hereby certified that *Amici Curiae* Joel Thayer and Meg Leta Jones are individuals and no person or entity owns them or any part of them.

/s/ Joel Thayer

Joel Thayer
Attorney of Record for *Amici Curiae*

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases:

Statutes & Other Authorities:

IDENTITY OF *AMICUS*, INTEREST IN THIS MATTER, AND SOURCE OF AUTHORITY TO FILE

Pursuant to Fed. R. App. P. 29(a), both amici are experts in the field of applying regulations to technology platforms.

Amicus Meg Leta Jones is a leading scholar of family technology policy. She is a Professor in the Communication, Culture, & Technology department, a founding faculty member of the Center for Digital Ethics, and a faculty fellow in the Institute for Technology Law & Policy at Georgetown University. In addition to her academic and popular press articles on technology governance issues impacting families, she is the author of *Ctrl+Z: The Right to Be Forgotten*, which examines the social, legal, and technical dynamics of digital oblivion, and *The Character of Consent*, which traces the transatlantic history of digital consent through the evolution of the internet "cookie." Prof. Jones earned her Ph.D. from the ATLAS Institute in the University of Colorado College of Engineering and Applied Science and a J.D. from the University of Illinois College of Law. Amicus encourages courts to properly weigh the ongoing harms to children and families from unregulated digital platforms when evaluating requests for preliminary injunctive relief.

Amicus Joel Thayer is President of the Digital Progress Institute, a Senior Fellow for AI and Emerging Technology Policy at the America First Policy Institute, a Senior Fellow at the Vanderbilt Policy Accelerator, and

a tech and telecom attorney. Mr. Thayer previously was an associate at Phillips Lytle LLP. Before that, he served as Policy Counsel for ACT | The App Association, where he advised on legal and policy issues related to antitrust, telecommunications, privacy, cybersecurity, and intellectual property. His experience also includes working as a legal clerk for FCC Chairman Ajit Pai and FTC Commissioner Maureen Ohlhausen and as a congressional staffer for the Hon. Lee Terry and the Hon. Mary Bono. He has testified before both the Senate Judiciary Committee on advancing a national privacy framework and the House Energy and Commerce Committee on protecting children online. His works have been featured in the *American University Intellectual Property Brief, Harvard Journal of Law and Public Policy*, *Yale Journal on Regulation, Stanford Technology Law Review, the Journal of American Affairs, The Wall Street Journal, Newsweek*, *The Hill*, *The National Review*, and *The Federalist Society*.

INTRODUCTION AND SUMMARY OF ARGUMENT

The sad reality of the digital age is that parents have been left on their own to fend off a tech-induced health crisis, contending against the allure of products engineered by the most powerful corporations in history to be maximally addictive to kids. Worse, Big Tech is not only indifferent to the harms children are suffering from its products, but there is also strong evidence that they intentionally

perpetuate the problem. *E.g.*, Aaron Tilley, *Apple's App Store Puts Kids a Click Away from a Slew of Inappropriate Apps*, The Wall Street Journal (Dec. 22, 2024), https://www.wsj.com/tech/apples-app-store-puts-kids-a-click-away-from-a-slew-of-inappropriate-apps-dfde01d5; *see also*, Joanna Stern, *How Broken Are Apple's Parental Controls? It Took 3 Years to Fix an X-Rated Loophole*, The Wall Street Journal (Jun. 5, 2024), https://www.wsj.com/tech/personal-tech/a-bug-allowed-kids-to-visit-x-rated-sites-apple-took-three-years-to-fix-it-17e5f65d.

That's why the law you are considering today, the App Store Accountability Act (S.B. 2420), is critical to ensuring parents can indeed parent in the digital age.

S.B. 2420 is premised on two simple principles: First, multi-trillion-dollar companies cannot (and should not) enter into sophisticated contracts or commercial relationships with minors without parental consent; and second, age-gating should be targeted at app stores to minimize the costs on parents, kids, adults, and app developers.

The first principle is straight-forward and historically grounded. As such, and unsurprisingly, in commercial transactions, the sellers and distributors are generally required to know whether they are engaging with a minor or at the very least know the identity with whom they are contracting. Applying that principle to this case: When you use an app store, you are entering into a contract via terms of service and privacy policies with Apple, Google, and third-party developers to

access a whole suite of digital products. And so S.B. 2420 regulates conduct, not content. The regulation is legally indistinguishable from any other commercial regulation.

To ensure its constitutionality, S.B. 2420 applies to all contracts minors may encounter on an app store, without singling out any particular service or content. This is a feature—not a bug—because it ensures that "[t]he legislation . . . [is] directed at unlawful conduct having nothing to do with . . . the expressive activity." *Arcara v. Cloud Books, Inc.*, 478 U.S. 697, 707 (1986). In this case, the State is making clear that its concerns rest with *any* company's formation of a contract with a minor without a parent or guardian's oversight. If the parent or guardian wants to allow their child to download an app or have no child restrictions at all on app downloads, S.B. 2420 would permit that.

This dovetails into the second principle. The framework was developed to rely on stakeholders' existing infrastructure and bottleneck so as to not reinvent the wheel. Indeed, placing the age-gating responsibility on app stores reduces the costs of age verification on parents, kids, adults, and app developers (large and small).

But how?

Every service goes through either one of two app stores—Apple's App Store and Google's Play Store. App store owners control every aspect of their app marketplace—and they oversee every time a user forms a contract by downloading

an app or making an in-app purchase. Setting the requirement at the app store level to verify the ages of users and communicate with the parents of minors removes the burden of every app developer from having to verify ages. It prevents every adult from having to go through yet-another age verification process whenever they access a new app. And it allows parents to decide what apps their kids can access, when they want to be notified, and otherwise set parental controls in one fell swoop.

In sum, S.B. 2420 is a conduct-based regulation and offers a light-touch framework leveraging the app stores' existing infrastructure to hand the reins over to parents to manage their child's digital experience.

ARGUMENT

I. Texas May Regulate Juvenile Commercial Relationships

Restricting adults from contracting with minors is a well-defined power of the state. The common-law infancy doctrine, "traced to the fifteenth century," renders any contract entered into by a minor voidable at the minor's option. Cheryl B. Preston & Brandon T. Crowther, *Infancy Doctrine Inquiries*, 52 Santa Clara L. Rev. 47, 47–48 (2012); *see also* Restatement (Second) of Contracts § 14 (Am. L. Inst. 1981).

Three durable propositions follow from the doctrine, each a fixture of American commercial law for centuries. *First*, minors are categorically different commercial

counterparties and the law has not treated them as full participants in the marketplace. *Second*, the States have historically intervened in minor-adult commercial dealings rather than leave them to ordinary arms-length contract law. And *third*, the burden has long fallen on the adult counterparty to know whom it is dealing with. As the Wisconsin Supreme Court put it, "adults dealing with minors must be deemed to do so in an awareness of the privilege the law affords the minor of disaffirming his contracts." *Kiefer v. Fred Howe Motors, Inc.*, 158 N.W.2d 288, 291 (Wis. 1968); *see also* 1 William Blackstone, *Commentaries on the Laws of England* 452 (1765) ("Infants have various privileges, and various disabilities: but their very disabilities are privileges; in order to secure them from hurting themselves by their own improvident acts.").

All States have some version of these rules. In Texas, for instance, a minor may open a bank account, but that account is subject to a parental or guardian veto to "deny the minor's authority to control, transfer, draft on, or make a withdrawal from the minor's deposit account . . . ." Tex. Fin. Code § 34.305(c). A minor may not sell "crafted precious metal" to a dealer without a "written statement from the seller's parent or legal guardian consenting to the transaction." Tex. Occup. Code § 1956.066. A minor generally may not enter into a life insurance contract unless approved by a "parent, grandparent, or adult sibling." Tex. Insur. Code § 1104.004. Texas even provides parents a "right to consent to the child's marriage, enlistment

in the armed forces of the United States, medical and dental care, and psychiatric, psychological, and surgical treatment." Texas Family Code § 151.001(6). In each case, the responsibility is on the bank, the dealer, the life insurance salesman, or the dentist to verify a person's age if they want a commercial relationship with that person to be valid.

As the Supreme Court wrote last year: "Requiring age verification is common when a law draws lines based on age." *Free Speech Coalition v. Paxton*, 606 U.S. 461, 478 (2025). The Court pointed to examples of how Texas requires "proof of age to obtain alcohol, tobacco, a tattoo, [or] a body piercing," *id.* at 480, and how federal law age-gates products and services, like the ability "to obtain certain medications from a pharmacist, . . . [or] employment as a minor," *id.* As the Court explained, "where the Constitution reserves a power to the States, that power includes 'the ordinary and appropriate means' of exercising that power." *Id.* at 478 (quoting J. Story, Commentaries on the Constitution of the United States § 430, at 412–413 (1833)). Age verification, the Court held, is just such an "ordinary and appropriate" means of enforcing the law.

What is more, that conclusion holds even where the regulated activity implicates a fundamental right or expressive activity. The *Paxton* Court explained that states may permissibly age gate activities such as issuing handgun licenses, registering to vote, or obtaining a marriage license. *Id.* In a similar vein, every State requires

parental consent (or imposes a categorical prohibition) before a minor may be tattooed, *see, e.g.*, 25 Tex. Admin. Code § 229.406—even though courts have held tattooing to be a "purely expressive activity" fully protected by the First Amendment, *Anderson v. City of Hermosa Beach*, 621 F.3d 1051, 1060 (9th Cir. 2010); *accord Coleman v. City of Mesa*, 284 P.3d 863 (Ariz. 2012) (en banc). And in *Ginsberg v. New York*, the Court upheld the conviction of a store owner for selling "girlie" magazines to a 16 year old without having made a "reasonable bona fide attempt to ascertain the true age" of the customer. 390 U.S. 629, 645.

Paxton makes clear that these precedents apply online. Per the Court, "requiring age verification online is plainly a legitimate legislative choice." 606 U.S. at 497. And so the age-verification statute at issue there, directed at websites purveying material obscene for minors, "simply adapts this traditional approach to the digital age." *Id.*

And following these precedents, Congress has intervened to protect minors in the digital commercial environment. The Children's Online Privacy Protection Act ("COPPA"), passed in 1998, requires operators of commercial websites and online services directed to children, or with actual knowledge of child users, to obtain "verifiable parental consent" before collecting personal information from any user under thirteen. 15 U.S.C. § 6502(b)(1); 16 C.F.R. § 312.3. The Federal Trade Commission has enforced COPPA for over twenty-five years, with settlements

totaling hundreds of millions of dollars, including the largest civil penalty ever obtained for an FTC rule violation, $275 million against Epic Games in 2022 for failing to obtain parental consent for data collection in *Fortnite*. *United States v. Epic Games, Inc.*, No. 5:22-cv-00597 (E.D.N.C. Dec. 19, 2022). In all of that time, no court has invalidated COPPA on First Amendment grounds.

Notably, there remains bipartisan interest in strengthening protections for children online. The bipartisan Children and Teens' Online Privacy Protection Act ("COPPA 2.0"), which passed the Senate in July 2024, would expand COPPA's reach to teenagers. S. 1418, 118th Cong. (2023) (Markey-Cassidy bill). And in early 2025, the FTC published a rule requiring separate opt-in parental consent before children's personal information may be disclosed to third parties for targeted advertising. Children's Online Privacy Protection Rule, 90 Fed. Reg. 16,913 (Apr. 22, 2025).

These same principles should decide this case. S.B. 2420's focus is fundamentally the same as these other commercial regulations that Texas has previously enacted and those the courts have reviewed. Applying age verification to contracting with minors falls well within a state's constitutional purview. When you use an app store, you are entering into a contract via and according to the terms of service and privacy policies with Apple, Google, and third-party developers to access a whole suite of digital products; indeed, Apple and Google both expressly say so. *See* Apple Media Services Terms and Conditions ("These terms and conditions create a contract

between you and Apple."); *See* Google Terms of Service (stating "Google services are provided by, and you're contracting with [] Google."). As such, S.B. 2420 adapts a centuries-old tradition of treating minors as different commercial actors to the primary digital platform through which commercial transactions now occur.

The State's concerns are primarily directed at a company's formation of a contract with a minor without a parent or guardian's oversight. Recall that in relevant part, S.B. 2420 requires app store owners, such as Apple's App Store or Google Play, to determine a user's "age category" using "commercially reasonable methods" at the time the user "creates an account" in the state, TX. Bus. Code § 121.021(a); "require that [a] minor's account be affiliated with a parent's" to ensure the parent can provide consent to the downloads and purchasing of mobile apps, *id.* § 121.022, and signal the age category (and parental consent, if a minor) to app developers, *id.* § 121.024. And as relevant to these provisions, an app store owner or app developer only violates the law if it "enforces a contract or a provision of a terms of service agreement against a minor that the minor entered into or agreed to without [parental] consent." TX. Bus. Code § 121.026(a)(1); *id.* § 121.056(a)(1).

Or to put it another way, the law adds a front-end authorization layer at the point where these commercial relationships actually form, leaving every minor's existing common-law right of disaffirmance intact and placing parents in the position COPPA has placed them in for over a quarter-century. Texas has traditional authority over

commercial transactions with minors, and S.B. 2420 "simply adapts this traditional approach to the digital age" through "ordinary and appropriate means" of age verification and parental consent. *Paxton*, 606 U.S. at 478.

II. S.B. 2420 Regulates Conduct, Not Content

As the Supreme Court held in *Arcara v. Cloud Books, Inc.*, when "[t]he legislation . . . [is] directed at unlawful conduct having nothing to do with . . . expressive activity," the First Amendment is not implicated. 478 U.S. 697, 707 (1986).

Here, S.B. 2420 is primarily directed at the conduct of technology company (whether an app store owner or app developer) forming and enforcing a contract with a minor without the parent's consent—not any expressive activity. As such, it should easily survive First Amendment scrutiny.

The District Court, nonetheless, found the S.B. 2420 to violate the First Amendment and issued a preliminary injunction. *CCIA v. Paxton*, 814 F.Supp.3d 787, 800-01 (W.D. TX 2025). Its holding was clear error.

First, the District Court ignored the text of the statute. As the District Court put it, "[a]n app store that fails to enforce the State's restrictions may face penalties of up to $10,000 per violation under the Texas Deceptive Trade Practices Act." *Computer & Communication Industry Ass'n v. Paxton*, 814 F.Supp.3d 787, 798 (W.D. Tex. 2025) (citing Tex. Bus. & Com. Code §§ 121.022(g), 121.053(b),

17.01, 17.46). Not so. S.B. 2420 only makes a "violation of this chapter" a deceptive trade practice, TX. Bus. Code § 121.101—and the law limits what constitutes a "violation" to enforcing a contract against a minor. TX. Bus. Code § 121.026(a)(1); *id.* § 121.056(a)(1).[1]

In other words, S.B. 2420 does not bar a minor from downloading or purchasing any app or making any in-app purchase nor does it bar any adult from doing the same. Indeed, it does not even bar an app store owner or app developer from enforcing a contract with an adult without having complied with the act's provisions. The law does not make "fail[ure] to enforce the State's restrictions" a violation of the Texas Deceptive Trade Practices Act. The only relevant violation is enforcing a contract against a minor without following the requirements of the law.

Recall that the District Court found that the plaintiff (CCIA) has standing because they are the "object" of the regulation and "face substantial liability." *Paxton*, 814 F.Supp.3d at 798-99. If that is true, it is only because CCIA's app-store-owner and app-developer members seek to enforce contracts against minors—which is precisely the sort of commercial activity that states have had the ability to regulate.

[1] To be clear, the act also prohibits an app store owner from "obtain[ing] a blanket consent to authorize multiple downloads or purchases" along with knowingly misrepresenting information to consumer and improperly sharing personal data—and contains several safe harbors to narrow potential liability. See TX. Bus. Code § 121.026; *id.* § 121.056. Those particular violations do not appear to be at issue in the District Court's holding.

Second, the District Court's holding was premised on its finding that S.B. 2420 was content-based and thus subject to strict scrutiny. That finding was improper.

Subject to two narrow exceptions, S.B. 2420 seeks to regulate all app-based contracts. It does not target only apps that themselves target children. It does not target only apps that are reasonably anticipated to be accessed by children. It does not target apps that have specific addictive qualities nor only those the legislature found to be harmful to children. As the text indicates, the law is indifferent to whether a child is downloading a Bible app or TikTok. If the app has a terms of service or privacy policy (or otherwise is creating a contract with a user), then the app store owner must verify a user's age and seek parental consent (and the app developer must receive the age category and such consent) if they ever intend to enforce those terms of service or privacy policy or other contract terms on a minor. If the parent or guardian wants to allow their child to download or purchase *any* app or make *any* in-app purchase, S.B. 2420 would permit that. The only requirement is that a parent, not a minor, consents to the commercial relationship if it is to be enforced.

The District Court apparently recognized the broad contours of the law, noting that it encompasses "apps that seek to promote physical or mental health, such as mindfulness apps like Calm, fitness apps like Strava, or therapy providers like BetterHelp." *CCIA*, 814 F.Supp.3d at 801. Indeed, it "does not limit its scope to

apps that use addictive algorithms designed to encourage prolonged use, or apps that are responsible in particular for causing excessive screen time." *Id.*

And yet, the District Court held the law to be "content-based" because it contained two narrow exceptions. And those exceptions are indeed narrow—they only absolve an app store owner from obtaining parental consent before allowing a minor (a) to download an emergency services app or (b) to download or purchase certain college-entrance apps otherwise regulated by state law. *See* TX. Bus. Code § 121.022(h). Notably, there is no similar exception for the developers of such apps—and so those app developers bear the risk of not being able to enforce a contract with a minor if their app is downloaded (or purchased) without parental consent.

Both exceptions address practical realities in which a minor may have a pressing need for immediate access to an app. The emergency services exception is obviously so—if a minor on an iPad encounters an emergency such as a fire or threat of violence, they may need immediate access to emergency services. And if a high school student needs access to a College Board app to take the SATs (and has forgotten to download it before the time for the test), they can nonetheless download the app and take the test without endangering their future education (at least in cases where the app is otherwise regulated under the state's education code). And again, in each case, the app developer has no exception—and so they

cannot enforce their terms of service or privacy policy against the minor unless and until they get parental consent.

We are not aware of any case in which a court has found an emergency exception to a general rule to transform that rule into a content-based regulation. Indeed, federal law is replete with such exceptions, including where the law directly regulates commercial communications. *See, e.g.*, 47 U.S.C. § 222(c)(1) (prohibiting a telecommunications carrier from "disclos[ing]" certain information about its customers); *id.* § 222(d)(4) (creating an exception for the disclosure of call location information in emergencies). Nor are we aware of any case in which a court has found an exception to a general rule based on other regulations to transform that rule into a content-based regulation. *See, e.g.*, 15 U.S.C. § 45(a)(1) (banning "unfair or deceptive acts or practices in or affecting commerce"); *id.* § 45(a)(2) (creating exceptions for a variety of otherwise regulated entities).

What is more, the Supreme Court has held that limited exceptions do not transform an otherwise content-neutral statute into a content-based regulation. Consider *TikTok v. Garland*, in which the Court reviewed a law that required divestitures for apps owned or controlled by certain foreign adversaries, with an exception for "an entity that operates a website, desktop application, mobile application, or augmented or immersive technology application whose primary purpose is to allow users to post product reviews, business reviews, or travel

information and reviews." Pub. L. No. 118-50, div. H, 138 Stat. 895, 955-60 (2024). The Court held that the law was content neutral even with that exception. 604 U.S. 56, 73 (2025).

In the same vein, the mere presence of an exemption or differential treatment does not necessarily transform a law that regulates conduct into a content-based regulation. In *City of Austin*, the Supreme Court found that the city's law as facially neutral even though the law distinguished between "off-premises" and "on-premises" signs. *City of Austin, Texas v. Reagan National Advertising of Austin, LLC*, 596 U.S. 61, 72 (2022). The Court distinguished the law's treatment from the one in *Reed v. Town of Gilbert* where the Court held that Arizona's sign code was content based because it gave favorable treatment to "ideological" signs than "political" signs. 567 U.S. 155, 159-60 (2015). In other words, as the Court in *Reed* explained, the difference must "depend *entirely* on the communicative content" for the exception to become content-based, 576 U.S. at 164 (emphasis added), and that is not the case here. The differential treatment here is premised on the practical realities of an emergency and preexisting regulation—and they only marginally impact the law's scope given that they apply only to app store owners, not app developers.

Even so, if this court believes that the law's exceptions make it content-based, it should have severed them from the statute rather than enjoin the entire law. The

Supreme Court has held that "when confronting a constitutional flaw in a statute, [judges] try to limit the solution to the problem, severing any problematic portions while leaving the remainder intact." *Free Enterprise Fund v. Public Company Accounting Oversight Bd.*, 561 U.S. 477, 508 (2010). Taking these exceptions out would be both prudent and a well within the purview of traditional severability principles. *Barr v. American Association of Political Consultants, Inc.*, 591 U.S. 610, 623-29 (2020). The District Court erred in not finding these exceptions could be severed, reasoning only that they were "part of the overall balance" struck by the legislature. *Paxton*, at 801. Such could be said of literally every provision in every law, which would make the doctrine of severance a nullity. What is more, there is no question that the legislature wanted to sever these provisions if necessary, as that is the entire point of the severability clause. S.B. 2420, § 2 ("It is the intent of the legislature that every provision, section, subsection, sentence, clause, phrase, or word in this Act, and every application of the provisions in this Act to every person, group of persons, or circumstances, is severable from each other.").

Third, the District Court erred in finding S.B. 2420 both overinclusive and underinclusive—setting an impossible bar for any digital age-verification statute to meet.

On the one hand, the District Court claimed the law was overinclusive because it targeted (almost) all apps, "not a narrowly tailored subset of apps deemed, for example, harmful or addictive based on evidence," *Paxton*, at 802, and faults the law for sweeping in "apps that seek to promote physical or mental health, such as mindfulness apps like Calm, fitness apps like Strava, or therapy providers like BetterHelp," *Id.* at 801, as well as "a dictionary or weather app." *Id.* 802.

In other words, the District Court faults the law for *not* being content-based enough. Precedent teaches that such a road is much more rocky for the states. Consider the Parental Notification by Social Media Operators Act, Ohio Rev. Code § 1349.09(B)(1), which requires "operator[s]" of "online web site[s], service[s], or product[s]" that "target[] children," or are "reasonably anticipated to be accessed by children" to "obtain parental consent before allowing any unemancipated child under the age of sixteen to register or create an account on their platform." *NetChoice v. Yost*, 716 F.Supp.3d 539, 547 (S.D. Ohio 2024) (citations omitted). The district court in that case enjoined the legislation, finding the law to be a content-based regulation because it "certainly requires consideration of the content on an operator's platform [because the State had] to determine if [the website] 'targets children' or is 'reasonably anticipated to be accessed by children.'" *Id.* at 557.

Or consider the Supreme Court's treatment of a California law that prohibited "the sale or rental of 'violent video games' to minors." *Brown v. Entertainment Merchants Ass'n*, 564 U.S. 786, 790 (2011). The Court grappled with the question of whether it was appropriate for the State to create a new category of obscenity, in this case "violent content." *Id.* at 793. And the Court ultimately struck down the law, finding it a content-based regulation.

In other words, the district court puts the state in a Catch-22: To avoid being overinclusive, the law must be content-based, which means strict scrutiny will apply, which means it is unlikely to survive judicial review. That cannot be the law.

On the other hand, the district court also faults S.B. 2420 for being underinclusive because "the same content offered via apps remains available to minors via pre-downloaded apps like Safari (or in stores)." *Paxton*, at 802. But it is hard to see, given the commercial-relationship focus on the law, how this is a fault.

For one, underinclusiveness is a problem because it "raises serious doubts about whether the government is in fact pursuing the interest it invokes, rather disfavoring a particular speaker or viewpoint." *Brown*, 564 U.S. at 802. The fact that "the same content . . . remains available to minors" only highlights the fact that nothing in S.B. 2420 is directed at regulating content. And the targeting of app stores and apps is intentional as it is the creation of an app store account and the downloading of an app that cements the commercial relationship between a user

and the app store owner or app developer. In other words, for the actual purposes of the law, it is not underinclusive at all.

For another, this admission by the court undercuts all of the supposed harms flowing from the law—how can S.B. 2420 possibly "cut[] teenagers off from wide swaths of the critical 'democratic forum[] of the Internet'"? *Paxton*, at 802. Or how could it "prohibit[] minors from participating in the democratic exchange of views online"? *Id*. The short and obvious answer is, it cannot.

For yet another, consider the supposed remedy for this "defect"—if the state of Texas wants to impose a parental-consent-based framework on the app stores and app developers and not be "underinclusive," then it must also impose that same framework on every website on the Internet. There is no law and no precedent that prohibits a state from proceeding incrementally or addressing the specific problem before it. Indeed, incrementalism in legislation is usually a virtue.

Fourth and finally, the District Court found S.B. 2420 to be a content-based regulation because it "sought to shield minors from certain speech the State deems objectionable or harmful," including apparently "targeted advertising." *Id*. at 800 But an alleged, partial content-based intent—especially one absent from the face of the legislation (the only mention of advertising in the entire law is a requirement to notify parents when advertisements are added to an app previously had none, *see* TX. Bus. Code § 121.053(b))—does not make a law a content-based regulation.

The *TikTok* Court upheld the TikTok divestment law "Even assuming [one of the law's] rationale[s] turn[] on content . . . ." *TikTok v. Garland*, 604 U.S. 56, 80-81 (2025). When a law's primary justification is not content-based—as the commercial-relationship regulation is not here as evidenced by the face of the law itself—an ancillary justification that considers content does not transform the law into a content-based regulation.

To be sure, the law fits more neatly as a standard consumer protection regime, especially when the court considers what Apple and Google both promise to the consumer. All S.B. 2420 seeks to do is to apply a standard consumer protection regime to hold these companies accountable when they intentionally fall short on those existing obligations and to what they claim in their own terms of services and privacy policies.

III. S.B. 2420 Is Narrowly Tailored to Accomplish Its Goals Because It Leverages the Bottlenecks of the Mobile Ecosystem

Apple and Google own all layers of your device. Apple controls its devices, operating system, and app store, while Google manages its operating system, app store, and major apps like YouTube, Search, and Chrome. Almost every app is accessed through either Apple's App Store or Google's Play Store. These stores manage every downstream commercial relationship we have with developers.

By requiring age verification and parental consent at the app-store level, S.B. 2420 simplifies these processes for the entire ecosystem, relieving app developers,

adults, parents, and children from repeated verification requirements and consent. As Jonathan Haidt rightly put, "with device-based verification *nobody else is inconvenienced*." Jonathan Haidt, *The Anxious Generation: How the Great Rewiring of Childhood Is Causing an Epidemic of Mental Illness*, p. 239 (2024). A parent verifies their child's device once with the app store and they're done. "[T]he internet is unchanged for them," *id.*, and they are still able to control what their kids see and do on their devices.

Even many of CCIA's own membership agree. In an amicus brief for the lower court, several of CCIA's members described the law's requirements as "technically feasible and commercially reasonable." *See* Amicus Curiae Brief of Coalition for a Competitive Mobile Experience, Case No. 1:25-cv-01660-RP, Doc. 58-1 at p. 6. They explain that the "'commercially reasonable' standard, safe harbors for widely adopted industry practices, and reliance on age categories the app stores themselves promoted in other jurisdictions further confirm that this is an incremental compliance project, not a ground-up re-architecting of the mobile ecosystem." *Id.* at 5.

What is more, the Supreme Court has found that nowadays age verification is a "modest burden" even when applied to dozens and dozens of websites. *Free Speech Coalition*, 606 U.S. at 464. It is certainly a modest burden for Apple and Google.

First, Apple and Google already tether child accounts to a parent account, consistent with the law's obligations. *See* Apple, *Family Disclosures for Children*, Privacy Policy, https://www.apple.com/legal/privacy/en-ww/parent-disclosure/ (last visited May 15, 2026).

Second, Apple and Google already require information about each user's age to create an account. Google verifies ages with a credit card or government ID. Google, *Access Age-Restricted Content & Features*, Google Account Help (last visited May 15, 2026), https://support.google.com/accounts/answer/10071085. Apple states that it does age verification through a variety of means, including (1) an ID in the user's digital wallet, (2) through parent-assisted age verification upon account creation, or (3) by providing the last four digits of a Social Security Number in addition to the information that these companies already have from the Device ID login. Apple, *Family Disclosures for Children*, Privacy Policy, https://www.apple.com/legal/privacy/en-ww/parent-disclosure/ (last visited May 15, 2026). And Apple already requires a user to provide "a government-issued ID in limited circumstances, including when setting up a wireless account and activating [a child's] device, for the purpose of extending commercial credit, managing reservations, or as required by law." Apple, *Apple Privacy Policy*, Apple (last updated Jul. 30, 2025), https://www.apple.com/legal/privacy/en-ww/.

Third, Apple and Google already communicate this age information to apps with their "Verify" programs. These Verify programs can be seamlessly integrated into apps and communicate only minimally necessary information securely through cryptographic signatures. Apple Developer, *Get Started with the Verify with Wallet API*, Wallet (last visited Apr. 1, 2026), https://developer.apple.com/wallet/get-started-with-verify-with-wallet/; Google, *Verify with Google Wallet*, Google Wallet (Apr. 1, 2026), https://developers.google.com/wallet/identity/verify.

Fourth, Apple and Google already manage parental consent mechanisms through their app stores and associated APIs. Apple's App Tracking Transparency ("ATT") feature *requires* developers to petition Apple when attempting to seek the consent of their users. Seb Joseph, *The Rundown: Apple's ATT Privacy Crackdown, a Year on*, DIGIDAY (Apr. 26, 2022), https://perma.cc/NR34-PEP2. Google offers a similar feature by default, although it does allow users to circumvent the feature. Google, *Change App Permissions on Your Android Phone*, Google Play Help (last visited Apr. 1, 2026), https://support.google.com/googleplay/answer/9431959.

None of this should be surprising, as the Federal Trade Commission already requires Apple and Google to seek parental consent for in-app purchases as a result of consent decrees. Federal Trade Commission, *FTC Approves Final Order in Case About Google Billing Kids' In-App Charges Without Parental Consent*, (Dec. 5, 2014), https://www.ftc.gov/news-events/news/press-releases/2014/12/ftc-approves-

final-order-case-about-google-billing-kids-app-charges-without-parental-consent; F.TC., *FTC Approves Final Order in Case About Apple Inc. Charging for Kids' In-App Purchases Without Parental Consent*, (Mar. 27, 2014), https://www.ftc.gov/news-events/news/press-releases/2014/03/ftc-approves-final-order-case-about-apple-inc-charging-kids-app-purchases-without-parental-consent.

Fifth, Apple and Google both claim to use a user's age for various purposes. For example, Apple claims to prohibit children under the age of 13 from creating an Apple ID—a necessary step in accessing access the App Store. Apple, *Create an Apple Account for Your* Child, Website (last visited Apr. 1, 2026), https://support.apple.com/en-us/102617. And if a child user attempts to change their age to an adult, Google locks the user out until it can verify the user's age. Google, *Update Your Account to Meet Age Requirement*, Google Account Help (last visited May 15, 2026), https://support.google.com/accounts/answer/1333913.

In short, S.B. 2420 is not inventing a whole new age verification and parental consent scheme unknown to the digital ecosystem—it is instead putting guardrails on existing practices to ensure that no minor forms a commercial relationship with an app store owner or app developer without a parent's consent. No party has suggested a less intrusive means for protecting the rights of children and their parents.

Finally, the court should take note that Apple and Google are true bottlenecks in the mobile ecosystem. Courts consider the "special characteristic[s]" of the market when assessing whether a measure is narrowly tailored. *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622 (1994) ("*Turner I*"). Such factors include "the bottleneck monopoly power exercised by [] operators" and "the unique power that vertically integrated companies have in the [relevant] market." *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622 (1994) ("*Turner I*"); *see also Turner Broad. Sys., Inc. v. FCC*, 520 U.S. 180 (1997) ("*Turner II*"); *Moody v. NetChoice, LLC*, 603 U.S. 707, 795 (2024) (J. Alito, concurring) (noting that that courts may soon need to consider the "enormous power exercised by platforms like Facebook and YouTube as a result of 'network effects'" when deciding on firms' First Amendment protections); *U.S. Telecom Ass'n v. FCC*, 855 F.3d 381 (D.C. Cir. 2017) (Kavanaugh, J., dissenting from denial of reh'g en banc).

App store owners, like Google and Apple, control every aspect of their app marketplace. If Apple refuses to adhere to content controls set by a parent, that parent would likely need to not only get a new phone but would also have to swap out every one of Apple's devices (*e.g.*, iPad, iMac, MacBook, etc.) and migrate (somehow) all of their data stored in Apple's various services because Apple controls its devices' operating systems and many of the default services therein. Federal Communications Commission Chairman Brendan Carr even described

Apple as "the single choking point" of the mobile ecosystem. Hon. Brendan Carr, X Post, February 12, 2024, https://twitter.com/BrendanCarrFCC/status/1757145971295695226.

To the extent this court has any doubt on whether S.B. 2420's requirements are narrowly tailored to the interests of Texas and the families of Texas, this court should follow that tradition and recognize that legislative solutions appropriately tailored to the special circumstances of the mobile digital ecosystem warrant deference.

CONCLUSION

For the following reasons, the Court should rule in favor of Defendant—Appellant.

/s/ Joel L. Thayer

JOEL L. THAYER
Counsel of Record
THAYER, PLLC
1255 Union Street NE
Seventh Floor
Washington D.C. 20009
(760) 668-0934
jthayer@thayer.tech
Attorney for *amici curiae*

CERTIFICATE OF SERVICE

I hereby certify that on May 21, 2026, a true and correct copy of the foregoing Brief of Amici Curiae was served via electronic filing with the Clerk of Court and all registered ECF users.

May 21, 2026

/s/ Joel L. Thayer

JOEL L. THAYER
Counsel of Record
THAYER, PLLC
1255 Union Street NE
Seventh Floor
Washington D.C. 20009
(760) 668-0934
jthayer@thayer.tech
ATTORNEY FOR *AMICI CURIAE*

CERTIFICATE OF COMPLIANCE

This brief has been prepared using 14-point, proportionately spaced, serif typeface, in Microsoft Word. Excluding the parts of the brief exempted by Fed. R. App. P. 32(f), this brief contains 6199 words.

/s/ Joel L. Thayer

JOEL L. THAYER
Counsel of Record
THAYER, PLLC
1255 Union Street NE
Seventh Floor
Washington D.C. 20009
(760) 668-0934
jthayer@thayer.tech
ATTORNEY FOR *AMICI CURIAE*