THE CASE FOR APP STORES TO AGE GATE HARMFUL ONLINE PRODUCTS

JOEL THAYER*

Today's digital age requires parents 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. The concerns with respect to online harms are very well documented. Indeed, there are seemingly countless studies, congressional hearings, and lawsuits all pointing out the unique impact that tech services have on childhood development and their mental health.

The question resides on what to do about it given that it is unlikely that tech companies will proffer any genuine solutions to quell the concern. Worse, large tech companies, such as Apple, Google, Amazon, and Meta, may even be intentionally perpetuating the problem.[1]

Given this, a government solution is necessary even with various online child safety laws on the books. And, indeed, states have been the pointed tip of the spear on that front. Most of the state-based solutions impose safety measures on platforms. However, recent attempts to impose restrictions on kids' use of addictive online products, like social media, have been thwarted by courts for being too broad or vague making them liable for swallowing up protected adult speech in its wake.

Courts have prescribed a remedy to address that concern—age verification. But this too has created yet another problem for legislatures because, even when applying such age-verification requirements to websites, courts have still exerted significant reticence. As the Supreme Court held in *Reno v. ACLU*, the issue with the government imposing its stated age-restrictions is that the platforms had "no effective way to determine the identity or the age of a user who is accessing material through e-mail, mail exploders, newsgroups or chat rooms."[2]

NetChoice's—a trade association representing the largest tech companies—challenge to California's child privacy law demonstrates the problem. The law in that case would, in part, require the websites to age-gate their services. Generally, the California district court was skeptical that websites could perform such a measure while also avoiding a chilling effect on adult speech. The Court wrote that the "steps a 'business would need to take to sufficiently

* President of the Digital Progress Institute. The author's organization help design the App Store Accountability Act's legal and policy framework.

[1] *See e.g.*, Aaron Tilley, *Apple's App Store Puts Kids a Click Away from a Slew of Inappropriate Apps*, WALL ST. J. (Dec. 22, 2024), https://www.wsj.com/tech/apples-app-store-puts-kids-a-click-away-from-a-slew-of-inappropriate-apps-dfde01d5 [perma.cc/7FB2-5L6C]; *see also* Joanna Stern, *How Broken Are Apple's Parental Controls? It Took 3 Years to Fix an X-Rate Loophole*, WALL ST. J. (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 [perma.cc/4JDK-59QJ].

[2] 521 U.S. 844, 855 (1997).

estimate the age of child users would likely prevent both children and adults from accessing certain content.'"[3] This led the Court to find that such measures would "appear likely to impede the 'availability and use' of information and accordingly to regulate speech."[4]

However, a district court in Arkansas gave us a path forward on how to avoid this obstacle—go through the app stores. When issuing his opinion granting NetChoice's preliminary injunction to stay Arkansas's social media law's enforcement, Judge Timothy Brooks noted that:

> iPhones and iPads empower parents to limit the amount of time their children can spend on the device, choose which applications (e.g., YouTube, Facebook, Snapchat, or Instagram) their children can use, set age-related content restrictions for those applications, filter online content, and control privacy settings.[5]

With that guidance, the position of this paper is that app stores should be responsible for age-gating most of these services. The reality is that almost all aspects of the digital ecosystem go through two companies—*i.e.*, Apple and Google. Apple and Google have leveraged their extraordinary market power to control every aspect of the app economy.

That's why the App Store Accountability Act[6] (the "Act") that states, such as Texas, Utah, and Louisiana, have enacted may provide a meaningful solution to this underlying problem. Here, I discuss the policy and legal justifications for the Act and why it appears poised to be a solution that will survive constitutional scrutiny, especially with respect to the First Amendment.

I. WHY THE ACT IS WISE TO GO THROUGH THE APP STORES TO VERIFY AGE

To answer why app stores are in the best position to perform age verification, let us start with the obvious—Apple and Google have leveraged their extraordinary market power to control every aspect of the app economy. Indeed, both companies are under a slew of antitrust suits from consumers, developers, and even the Department of Justice and attorney generals for their monopolistic control over their stores and devices.[7] As Federal Communications Commission Chairman Brendan Carr has put it, app stores are "the single choking point" of the mobile ecosystem.[8] Thus, the Act leverages the mobile ecosystem's existing infrastructure to perform age verification, which eases compliance costs without diluting the Act's child safety objective.

But how?

Every service goes through either one of two app stores—Apple's App Store and Google's Play Store. App stores provide the front door to every addictive and harmful product to kids. A law requiring them to verify the ages of users and communicate with the parents of minors streamlines the process. This measure also removes the burden of every app developer from

[3] *NetChoice v. Bonta*, 692 F. Supp. 3d 924, 945 (N.D. Cal. 2023), *aff'd in part, vacated in part*, 113 F.4th 1101 (9th Cir. 2024).

[4] *Id.* at 946.

[5] *NetChoice v. Griffin*, 2023 WL 5660155, p. *7 (W.D. Ark 2023).

[6] S. 1586, 119th Cong. (2025).

[7] Compl., *United States v. Apple Inc.*, No. 2:24-cv-04055, (D.N.J. Mar. 31, 2024), https://www.justice.gov/d9/2024-03/420763.pdf [perma.cc/FF84-7YNP]; Pls. Opening Statement, *United States v. Google LLC* (E.D. Va. Apr. 17, 2025), https://www.justice.gov/d9/2023-09/416684.pdf [perma.cc/X4KT-ZFNS].

[8] Hon. Brendan Carr (@BrendanCarrFCC), X (Feb. 12, 2024), [perma.cc/44A2-2FQV].

having to verify ages, and every adult from going through yet-another age verification process whenever they access a new app.

It's clear that app stores already have methods to verify a child's parent or legal guardian, and can more accurately estimate the user's age either through an ID placed in the user's digital wallet, parent-assisted age verification upon account creation, or a requirement to provide the last four digits of your SSN in addition to the information that these companies already have from the Device ID login. Better yet, they can accomplish all of these without the use of facial scans or other biometric markers.

Additionally, both companies not only have created age verification procedures but have also pushed the consent mechanisms and app monitoring away from the developers and to their stores. For instance, Apple has already pushed age verification and consent mechanisms through its App Store via its App Tracking Transparency ("ATT") feature.[9] Apple's ATT, in spirit, is an attempt to bring more transparency on what apps collect on users while they are on their Apple device. Practically, this feature means that developers must petition Apple when attempting to verify the age of their users or find a user engaging in illegal activities occurring in their app (e.g., botnet attack, sex trafficking, or moderation of child pornography). To make such operations functional, Apple must already approve every interaction between developers and iOS users.

The same is true for Google Play. Google allows consumers to circumvent consent protocols from the app to the Play Store.[10] Indeed, both Apple and Google maintain almost exclusive control over developers' relationship with their customers, which make developers further rely on Apple, Google, and their services. Apple and Google's developer guidelines—which are actually contractual terms—also require all developers to run every aspect of their business by them first.[11] The Ninth Circuit found that with respect to Apple, in particular: "Developers can distribute their apps to iOS devices only through Apple's App Store and after Apple has reviewed an app to ensure that it meets certain security, privacy, content, and reliability requirements."[12] Google's Play Store operates in an almost identical way.

Google and Apple's control is especially present in age verification and parental consent protocols. Apple already says so in its own policy concerning child accounts and provides a slew of options for users to verify their ages in certain jurisdictions. It states:

> Apple may take additional steps to help verify that the user granting permission for the creation of a child's Apple ID is their parent or legal guardian. Accordingly, in these jurisdictions, you may be asked to verify your current iTunes, iCloud, or Apple Store payment method. Depending on the payment method, this can be done using the security code from your credit card or a similar verification method. Alternatively, you may have the option to verify your age using your identity card in Wallet or verify using your Apple ID account.[13]

---

[9] Seb Joseph, *The Rundown: Apple's ATT Privacy Crackdown, a Year on*, DIGIDAY (Apr. 26, 2022), [https://perma.cc/NR34-PEP2].

[10] *Change App Permissions on Your Android Phone*, GOOGLE PLAY HELP (last visited Jun. 15, 2025), https://support.google.com/googleplay/answer/9431959?hl=en [perma.cc/RY2W-GFEA].

[11] *Epic Games, Inc. v. Apple*, 67 F.4th 946 (9th Cir. 2023).

[12] *Id.* at 967.

[13] *Family Privacy Disclosure for Children*, APPLE (last visited Jun. 15, 2025), https://www.apple.com/legal/privacy/en-ww/parent-disclosure/ [perma.cc/LX7E-K9ZH].

Also in those jurisdictions, Apple even requires the 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."[14] Google also age verifies with a credit card or government ID.[15] If any user changes their age and that changes the adult status, Google locks the user out until it verifies the user's age.[16]

The reason they have these measures in place is due to Apple and Google's respective age limits for their products. Apple prohibits children under the age of 13 to create an Apple ID—something necessary to access the App Store.[17] To reiterate, Apple requires the adult users to verify their age by adding either a credit card or a government ID to create an Apple ID for a child.[18] Upon device setup, each user is required to input their birth date. Currently, children under 13 are required to have a parent assist with account creation, including being aware of the stated birth date. Birth dates can't be changed by the child. Google has similar restrictions

Not only does Apple and Google maintain all the technical controls and direct access to the age data, but both companies are subject to consent decrees administered by the Federal Trade Commission ("FTC") that requires both app store providers to obtain parental consent before either of them can approve any purchase by children within their app stores. According to the FTC, its order "requires Google...to modify its billing practices to obtain express, informed consent from consumers before billing them for in-app charges."[19] Apple's consent decree, too, has the same provision. Indeed, the FTC's consent decree requires "Apple [to] change its billing practices to ensure that... [it] obtain[s] express, informed consent from consumers before charging them for in-app purchases."[20] Hence, both theoretically must have age-verifiers in place to comply with their FTC orders. All the Act asks Apple and Google to do is to use those same Application Programming Interfaces—the software protocols and rules that allows apps to communicate with other apps on a mobile device—for app downloads.

These facts have informed and are reflected in the Act's enforcement. Indeed, the federal version of the Act allows the FTC to evaluate a slew of options to achieve app-store age verification through a guidance document as opposed to outlining prescriptive technology requirements in the statute itself.[21] This is wise for two reasons: (1) We do not want the statute to exclude technical advances that can be construed as the least restrictive means; and (2), frankly, technology changes and, when it does, the agency can reevaluate what a "commercially available" method means at that point. This better ensures, in my view, the statute's

---

[14] Apple Privacy Policy (last visited Jun. 15, 2025), https://www.apple.com/legal/privacy/en-ww/.

[15] Google Help Center (last visited Jun. 15, 2025), https://support.google.com/accounts/answer/10071085?hl=en.

[16] Google Help Center "Update your account to meet age requirements" (last visited Jun. 15, 2025), https://support.google.com/accounts/answer/1333913?hl=en.

[17]Apple Create an Apple Account for Your Child Policy (last visited Jun. 15, 2025), https://support.apple.com/en-us//102617#:~:text=To%20verify%20that%20you're,added%20to%20Wallet%20where%20available.

[18] *Id*.

[19] Federal Trade Commission, *Press Release: FTC Approves Final Order in Case About Google Billing Kids' In-App Charges Without Parental Consent* (Dec. 5, 2014), ftc.gov/news-events/news/press-releases/2014/12/ftc-approves-final-order-case-about-google-billing-kids-app-charges-without-parental-consent [perma.cc/Q76S-TN5W].

[20] Federal Trade Commission, *Press Release: FTC Approves Final Order in Case About Apple, Inc. Charging for Kids' In-App Purchases Without Parental Consent* (Mar. 27, 2014), ftc.gov/news-events/news/press-releases/2014/03/ftc-approves-final-order-case-about-apple-inc-charging-kids-app-purchases-without-parental-consent [perma.cc/C8ZQ-HQAY].

[21] App Store Accountability Act, S. 1586, 119th Cong., 1st Sess., § 5 (2025).

constitutionality, gives the Act more regulatory flexibility, and avoids being overly limited in scope.

In sum, given that Apple and Google both have a Herculean grip over their app stores, already control all of their parental features, already approve and validate app purchases, already have direct access to the device's wallet, and have pushed all consent protocols to their stores, placing the consent and age verification responsibilities on them is just an obvious avenue. It is why the Act's having app store providers do the bulk of the age verifying makes perfect sense.

II. THE ACT'S USE OF AN AGE API, OR SIGNAL, BETTER ENSURES USER PRIVACY

The Act specifically requires app store providers to safeguard age data. What is more, the Act makes it unlawful for developers to use or sell any of the age data collected or received from app store providers. Developers are only able to use the data to comply with their respective obligations.

But even if that isn't enough, the Act does not require Instagram, TikTok, or Snap to collect a photo of the user's driver's license or, as experts have testified to in open court, [22] require a third-party verifier.

The Act ameliorates this privacy concern because, as discussed at length above, it is well documented that the app stores already have all this age information. This means that the user would not need to proffer more data to these platforms—a distinct characteristic from website-level age verification requirements.

Indeed, the Act merely asks app store providers to send a "signal" to developers when they suspect a child is using their app or service without burdening the user by requiring more personal data. All the proposed law would require is for Apple and Google to give the app a digital "thumbs up" or "thumbs down" when an app asks to verify the device is owned by an adult or a child. This signal ensures that neither a user's ID nor a third-party verifier would be necessary for app store providers or developers to comply with the Act, while also not having websites or developers ask for more personal information from users.

But why is a signal more privacy focused? App stores already can anonymously 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.

In Apple's policy for Verify with Wallet, it explains, "When you integrate with Verify with Wallet, . . . your app will be entitled to request only the specific data required to complete the transaction. This prevents users from having to overshare their identity information. Furthermore, neither the state issuing authority nor Apple can see when and where a user shares

[22] *NetChoice v. Griffin*, 2023 WL 5660155 *3 (W.D. Ark 2023) (admitting that "the user then would be shunted to a third-party servicer that collects official documents, such as digital identification cards or digital driver's licenses.").

their license or ID."[23] Google states that: "All data on the ID is backed with a cryptographic signature for secure and seamless verification."[24]

If we required websites to perform age verification alone, they would undoubtably ask users to upload a picture of their ID to each app or have them provide that data to another third-party vendor. An app store signal presents a one-and-done solution for apps—users don't need to prove their age to each app, only prove it to the app store once. What's more, all of these social media companies set their age gate at 13, but none of them really enforce it.

Given that the Act treats the receipt of an age signal from the app store as a developer having "actual knowledge," the Act puts developers' policies to the test since they'd now be aware how many of their users are actually under 13 to better enforce COPPA and all without the consumer forfeiting more information to the likes of Meta or TikTok. It's a win-win.

III. LEGAL CONSIDERATIONS SUPPORTING THE USE OF APP STORE AGE VERIFICATION

The Act relies on a standard legal principle—multi-trillion-dollar companies cannot enter into sophisticated contracts with minors. Make no mistake, 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. The regulation is legally indistinguishable from any other commercial regulation. Mainly because, 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. Below, I expand on the legal considerations discussed above with a keen focus on tech companies's usual objection, *i.e.*, the First Amendment.

A. First Amendment Considerations

1. The Regulation is a Conduct Regulation, Not a Content Regulation

To ensure its constitutionality, the Act applies to all contracts minors may encounter on an app store, instead of singling out any particular service or content. It is why the fact that the Act applies to all apps is very much a feature and not a bug. This feature demonstrates to courts that "[t]he legislation . . . [is] directed at unlawful conduct having nothing to do with . . . the expressive activity."[25] In this case, the Act makes clear that the state is concerned with a company's ability to form a contract with a minor without a parent or guardian's oversight; it is unconcerned with preventing users (child or not) from accessing or engaging on a particular app outright. If the parent or guardian wants to allow their child to download an app or have no child restrictions at all on app downloads, the Act would permit that. Full stop.

This approach is distinct from what the state of Ohio attempted when it passed the Parental Notification by Social Media Operators Act ("Ohio Act").[26] The Ohio Act requires "operator[s]" of "online web site[s], service[s], or product[s]" that (1) "target[] children," or are "reasonably

[23] Apple Wallet Policy (last visited Jun. 15, 2025), developer.apple.com/wallet/get-started-with-verify-with-wallet/ [perma.cc/TC9J-W399].

[24] Google Wallet Policy (last visited Jun. 15, 2025), developers.google.com/wallet/identity/verify [perma.cc/76VK-J7PZ].

[25] *Arcara v. Cloud Books, Inc.*, 478 U.S. 697, 707 (1986).

[26] Ohio Rev. Code § 1349.09(B)(1).

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."[27] Specifically, the Ohio Act required a platform to "[o]btain verifiable consent for any contract with a child, including terms of service, to register, sign up, or otherwise create a unique username to access or utilize the online web site, service, or product, from the child's parent or legal guardian" through a variety of acceptable methods; and (2) present to the parent or guardian a list of features related to content moderation and a link where they may review those features."[28]

The Ohio Attorney General attempted to rely on the premise that "the [Ohio] Act does not regulate speech, simply the ability of minors to contract."[29] He further argued that "the legislation is concerned with operators' release of minors' personal information and data pursuant to exploitative terms of service, addictive social media features like 'infinite scroll,' increased rates of mental illness in children, and a risk of exposure to sexual predation on websites that facilitate private messaging between users."[30]

The Court disagreed with General Yost's justification because, at the outset, the Ohio Act was clearly seeking to regulate content, not the conduct of regulating contracts. Why? Because, for one, the Ohio Act excluded a whole host of other sites that have the same features and capabilities to collect a child's data.[31] Secondly, the Court held that the "[Ohio] Act . . . 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.'"[32] For these reasons, a court found this law a content regulation.

The Act here avoids this issue entirely and is likely to still be upheld as a conduct regulation. As previously stated, the Act seeks to regulate all contracts, not just ones that "target children" or are "reasonably anticipated to be accessed by children." Indeed, the Act is indifferent to whether a child is downloading a Bible app or TikTok. If the app has terms of service or a privacy policy, then it requires the app and the app store provider to seek parental consent after they have determined that the user is a child. As was the case with the law the Supreme Court reviewed in *City of Austin v. Reagan National Advertising of Austin, LLC*, the App Store Accountability Act does not "single out any topic or subject matter for differential treatment."[33] Thus, this type of regulation is closer to the health code violation in *Arcara* or the divestiture requirement in *TikTok v. Garland*.[34]

Indeed, this proposal leverages a standard policy prescription to prevent children from accessing addictive services or products—the onus is on the store to age gate the product. When you walk into a convenience store, we require the store to check for an ID when a patron purchases cigarettes, alcohol, and pornography. We also hold the store liable when kids access

[27] *NetChoice v. Yost*, 716 F.Supp.3d 539, 547 (S.D. Ohio 2024) (citations omitted).

[28] *Id.* at 554 n.3 (citing Ohio Rev. Code Ann. § 1349.09 (West)).

[29] *Id.* at 552.

[30] *Id.* at 554-55.

[31] *Id.* at 559 (explaining that "a child can still agree to a contract with the *New York Times* without their parent's consent, but not with Facebook.")

[32] *Id.* at 556.

[33] 596 U.S. 61, 71 (2022).

[34] *Compare* Arcara v. Cloud Books, Inc., 478 U.S. 697 *with* TikTok v. Garland, 145 S.Ct. 57 (2025).

those products, not necessarily the suppliers of the product. In other words, we don't rely on Philip Morris or Anheuser-Busch to ensure kids aren't purchasing their products; we look to CVS, 7-11, and supermarkets to age gate. What is more, we generally don't allow a child to obtain a bank loan without a parent present or at the very least require them to co-sign for the loan. The app ecosystem should be no different.

Moreover, enlisting app store providers to perform age verification balances the government's goal of providing parents the legal recourse to protect their children from harmful tech services, while not infringing on adults' online speech. Why is this the case? Well, as Jonathan Haidt rightly put, "with device-based verification *nobody else is inconvenienced*."[35] A parent verifies their child's device once with the app store and they're done. "[T]he internet is unchanged for them,"[36] and they are still able to control what their kids see and do on their devices.[37]

2. The Act's Age Rating Provisions Do Not Raise Compelled Speech Concerns Because it is a Transparency Requirement

Some may argue that the age rating provisions compels tech companies' speech. It is true that the Act requires apps to display an age rating and for apps to provide a general description of their app. In general, the First Amendment does not permit the government to force companies to host speech with which the company disagrees; otherwise, this would run afoul of the court-made compelled speech doctrine under the First Amendment.

The Act, however, does not require app store providers or developers to take a position on what speech is considered unsafe for kids. Instead, it requires that child-protection mechanisms be accessible, and the apps be transparent with their offerings through their provided app age ratings and content descriptions. Hence, it's unlikely that (or at least unclear how) the compelled speech doctrine applies here.

In general, courts evaluate First Amendment considerations concerning disclosure requirements under *Zauderer v. Office of Disciplinary Counsel*.[38] The Supreme Court in *Zaudere* views disclosure requirements as content neutral because their purpose is to disclose "purely factual and uncontroversial information" about their conduct toward their users and the "terms under which [their] services will be available."[39] The Supreme Court further clarified in *Milavetz, Gallop & Milavetz, P.A. v. United States* that while "restrictions on nonmisleading commercial speech regarding lawful activity must withstand intermediate scrutiny," when "the challenged provisions impose a disclosure requirement rather than an affirmative limitation on speech . . . the less exacting scrutiny described in *Zauderer* governs our review."[40] Additionally, a commercial disclosure requirement must be "reasonably related to the State's interest in

[35] JONATHAN HAIDT, THE ANXIOUS GENERATION: HOW THE GREAT REWIRING OF CHILDHOOD IS CAUSING AN EPIDEMIC OF MENTAL ILLNESS 239 (2024).

[36] *Id*.

[37] *Id*.

[38] 471 U.S. 626, 652 (1985).

[39] *Id* at 652.

[40] 559 U.S. 229, 249 (2010).

preventing deception of consumers" and must not be "[u]njustified or unduly burdensome" such that it would "chill[] protected speech."[41]

Even a more liberal Eleventh Circuit in *NetChoice v. Attorney General, Florida* held that Florida's social media law's disclosures (excluding the one requirement that platforms provide notice and a detailed justification for every content-moderation action) was likely to withstand a constitutional challenge. The Eleventh Circuit even identified Florida's "require[ments for] platforms to publish their standards . . ." as being part of that consideration.[42]

Here, the age-rating and descriptions requirements in the Act are informed by a fundamental principle in contract law—a party can only assent to terms they understand. Let's start with how the Act works in this respect. The age rating ultimately comes from the developer. All it requires from the app store provider is to display the developer's self-description. This framework borrows from myriad other consumer protection requirements and contract law, such as privacy laws or the Uniform Commercial Code. None of those regulations have raised First Amendment concerns.

The Act is also consistent with other child-privacy measures and proposals. For instance, COPPA, specifically Section 6502(a)(2), has nearly the same disclosure mechanism.[43] Like COPPA, the Act only asks the developers and app store providers to disclose what the app does, what type of content it hosts, and apply its app ratings consistently. What's more, because all developers and app store providers already have set age limits that have not materially affected their services in any conceivable way, they are likely not unduly burdensome. The Act even allows for a safe harbor in the event app store providers and developers use various industry standards, like MPA's movie ratings or the gaming industry's ESRB.

Given that all the bill does is ask the developers and app store providers to be transparent with their users, it is unlikely that these rules will be considered compelled speech.

* * *

In sum, the Act is a straightforward and practical approach to keep our kids safe online and give parents the empowerment they want and deserve.

[41] *Id.* at 230, 250.

[42] *NetChoice v. Attorney General, Florida*, 34 F.4th 1196, 1230 (11th Cir. 2022).

[43] *See* 15 U.S.C. § 6502(a)(2).