

**UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF ALABAMA**

COMPUTER &
COMMUNICATIONS INDUSTRY
ASSOCIATION,

Plaintiff,

vs.

STEVE MARSHALL, in his official
capacity as Attorney General of
Alabama,

Defendant.

Case No. _____

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

Plaintiff, the Computer & Communications Industry Association (“CCIA”), brings this civil action against defendant, Steve Marshall (in his official capacity as the Attorney General of Alabama), for declaratory and injunctive relief and alleges as follows:

INTRODUCTION

1. Alabama Act No. 2026-59 (HB161) (the “Act” or “Act 2026-59”) imposes a broad censorship regime on mobile app stores and apps. *See* Ex. A (text of Act). In a misguided attempt to protect minors, the Act requires proof of age before anyone with a smartphone or tablet can access any app store and download a

single app. Anyone under 18 must also obtain parental consent for every app download or in-app purchase—from ebooks to email to entertainment. At the same time, the Act could be read to require app developers to rate the age-appropriateness of their apps according to Alabama’s vague and unworkable set of age categories, provide app stores with a content description justifying those age categories, and then use those same categories to implement the apps’ safety-related features or defaults, such as content ratings for in-app media.

2. The First Amendment forbids laws that require businesses to “card” people before they can enter public libraries, bookstores, and community theaters. And that fundamental speech protection applies as much in cyberspace as it does in the physical world. *Packingham v. North Carolina*, 582 U.S. 98, 104 (2017). App stores make available a variety of mobile apps as broad as, or broader than, these traditional fora for speech. They allow users to access, create, and exchange an enormous quantity of speech, including current events, religious material, educational content, books, movies, short-form video, music, art, games, and much more.

3. There is no legitimate purpose for a law that interposes a state-mandated ID-check and parental-consent regime to limit access to this vast universe of protected speech. But to the extent any exists, the Act is simultaneously too overbroad and too underinclusive to achieve it. In fact, the Act is unnecessary: app

stores and app developers already provide parents with tools to help them control what their children can access on their mobile devices, thereby preserving parental choice without burdening access to protected expression for everyone. The Act's predominant effect, ironically, is therefore to *confine* parental choice by imposing a one-size-fits-all restriction on access to the multitude of app store offerings (including books, movies, and games), regardless of age and user (or parental) preference.

4. CCIA is a leading trade organization representing internet, technology, and communications companies. Its members include operators of app stores (like Google, Apple, and Amazon) and developers of mobile apps (like YouTube, Audible, Apple TV, IMDb, and Goodreads), all covered by the Act. CCIA members' app stores curate and publish apps that facilitate the exchange of vast amounts of protected speech for both minors and adults, along with countless life-enhancing tools and access to the world's knowledge, all through a mobile device. And CCIA members' apps collectively offer services for users to read, view, and create immense amounts of speech and information.

5. The Act prohibits all Alabamians from accessing mobile app stores at the threshold unless they first comply with invasive age-verification procedures that burden the free speech rights of the app stores, app developers, and their users. Mobile app stores and app developers are further barred from disseminating all but

a very select few apps to minor users without first complying with onerous parental-verification and parental-consent restrictions that further burden those rights.

6. These verification and consent mandates are the core features of the Act and impose burdens on accessing speech on mobile apps at three key chokepoints: (1) for all users at account creation and, for all minor users, (2) prior to downloading an app and (3) on an ongoing basis for all in-app purchases and every time an app significantly changes its policies.

a. *First*, all users, *regardless of age*, who wish to access apps on a mobile app store must submit to a burdensome and privacy-invasive age-verification process designed to sort users into one of several age-based categories, most likely by uploading a picture of their government IDs. § 2(a).¹ If a user cannot sufficiently demonstrate they are over 18 years old, the user must “affiliate[],” *i.e.*, link, their account to that of a parent or guardian, meaning a biological parent, legal guardian, or individual with legal custody, but only after the parent or guardian establishes they are over 18. §§ 1(15), 1(16), 2(b), 3(1).

b. *Second*, any user determined to be a minor is forbidden from downloading any mobile app—including mobile newspapers, bible

¹ Unless otherwise noted, statutory citations refer to Alabama Act No. 2026-59.

study apps, educational apps, messaging apps, or games—without first obtaining verifiable parental consent for that download. §§ 3(1), 3(2).

- c. *Third*, a verified parent must affirmatively consent to **each and every** purchase within an app (including books, music, TV shows, movies, games, and concert tickets), each of the minor’s subsequent downloads of any mobile apps, as well as vaguely defined “significant changes” to apps. §§ 3(2), 4(2)(b).

7. These requirements have far-reaching implications for protected speech. Under the Act, if a 45-year-old would like to access news apps available on the Google Play Store, he must first hand over personally identifying information to Google pursuant to the State’s mandatory age-verification process. And if a 16-year-old wants to download the Audible App in order to listen to audiobooks, she would first have to establish her own age; then she would have to tether her account to a parent’s, who would then need to establish their own age, identity, and relationship to the minor and provide consent for the minor to create her account; then, she would have to wait for the parent to provide consent for the app, and finally get separate parental consents for every single book title she wished to purchase via the app. The same is true for apps like ESPN, Wikipedia, Spotify, Audible, Substack, Duolingo, Goodreads, BibleProject, Atheism Pocket Debater, TED, Bandcamp, Merriam-

Webster Dictionary, Khan Academy Kids, Gabb Messenger, and on and on. Even worse, minors who do not have a parent or legal guardian able to provide consent under the Act will be entirely shut out of mobile app stores and the thousands of speech-enabling apps and the speech and information that apps provide. Even minors who can successfully link a verified parent account are burdened when their parents are (understandably) too busy to approve each and every request as it is made.

8. In short, instead of tailoring its reach, the law walls off virtually all mobile apps behind a series of verification and consent gates. That includes apps that facilitate core political or educational speech; creative or artistic expression; religious instruction and information; or the exchange of ideas, information, and culture. Alabama has “burn[ed] the house to roast the pig.” *Butler v. Michigan*, 352 U.S. 380, 383 (1957).

9. The Act also ignores less restrictive alternatives, including existing parental controls, many apps’ existing verification and consent tools tailored to particular services within those apps, and Alabama’s targeted obscenity laws, *see* Ala. Code § 8-19G-3 (2025) (requiring age verification for accessing pornography on the internet), while appearing to impose standardless, compelled-speech requirements that dismantle established industry safety frameworks.

10. The Act is subject to strict scrutiny because of its content-based purpose. The legislative record—including statements from sponsors in both the

House and Senate, as well as other representatives and senators—makes clear that the Act is justified by the desire to protect minors from content the state deems harmful or age-inappropriate.

11. Given the Legislature’s purpose, the State cannot avoid strict scrutiny by applying the Act’s age-verification and parental-consent mandates broadly to wall off access to “an entire medium of expression,” *City of Ladue v. Gilleo*, 512 U.S. 43, 55 (1994)—and one that involves a vast array of speech that is fully protected by the First Amendment as to both minors and adults.

12. Even if the Court were to apply intermediate scrutiny, the Act could not withstand constitutional muster, because it is not at all tailored to serve any interest, including the State’s purported interest in “protecting children online.” *Debate on H.B. 161 Before the Ala. House of Rep.*, 2026 Reg. Sess., at 27:13–19 (Jan. 22, 2026) (statement of Rep. Chris Sells), <https://alabamachannel.ompnetwork.org/embed/full/sessions/1216?embedInPoint=0&embedOutPoint=0&shareMethod=link>.

13. The Act also violates the Commerce Clause by excessively burdening interstate commerce in relation to the purported local benefit conferred on the State of Alabama. The Act forces national platforms to dismantle uniform operations in favor of Alabama-specific mandates, forces app stores to comply with an inconsistent patchwork of state rules across the United States, and effectively

regulates commercial and speech-related activities that occur wholly outside Alabama. This compelled fragmentation balkanizes the digital marketplace—impermissibly projecting Alabama’s idiosyncratic regulatory scheme onto the national economy while failing to provide a constitutionally permissible or effective local shield.

14. The Court should declare the Act unconstitutional and enjoin its enforcement as to CCIA’s app store and developer members.

PARTIES

15. Plaintiff CCIA is a non-profit organized under Section 501(c)(6) of the Internal Revenue Code incorporated in the Commonwealth of Virginia. For more than 50 years, CCIA has promoted open markets, open systems, and open networks.

16. Based on the Act’s definitions, the Act regulates and significantly burdens CCIA’s members both in their capacity as app store owners and app developers, including: (1) Google, which owns and/or operates the Google Play Store, Google Search, Gmail, and Google Maps, among others; (2) Amazon, which owns and/or operates the Amazon Appstore, Audible, IMDb, and Goodreads, among others; and (3) Apple, which owns and/or operates the Apple App Store, Apple TV, Apple News, and Apple Music, among others. Google, Apple, and Amazon “own[], operate[], or control[] . . . app store[s],” defined as a “publicly available website, software application, or electronic service that allows account holders to download

apps from third-party developers onto a mobile device.” § 1(6)–(7). Numerous other CCIA members also develop mobile apps that are regulated by the Act. *See* § 1(5) (defining “app” as “a software application or electronic service that a user may run or direct on a mobile device,” including pre-installed apps); § 9 (imposing requirements on “developers” of applications).

17. Defendant Steve Marshall, the Alabama Attorney General, is a resident of Alabama and is named in his official capacity.

STANDING

18. CCIA has standing to challenge the Act on multiple grounds.

19. CCIA has associational standing because (1) some of CCIA’s members have standing, as those members are “the object” of the Act’s regulation and face substantial liability, *Diamond Alternative Energy, LLC v. EPA*, 606 U.S. 100, 112 (2025); (2) challenging the Act is germane to CCIA’s mission; and (3) CCIA members’ individual participation as parties is unnecessary in this purely legal challenge, *Baughcum v. Jackson*, 92 F.4th 1024, 1031 (11th Cir. 2024); *Arcia v. Fla. Sec’y of State*, 772 F.3d 1335, 1342 (11th Cir. 2014).

20. *First*, CCIA has standing to bring a pre-enforcement challenge against the Act because its members are indisputably engaged in conduct that is “affected with a constitutional interest ... that is proscribed by” the Act. *CCIA v. Uthmeier*, No. 25-11881, 2026 WL 3071065, at *4 (11th Cir. Oct. 14, 2026); *Fla. State Conf.*

of *N.A.A.C.P. v. Browning*, 522 F.3d 1153, 1160–62 (11th Cir. 2008) (imminent harm to members sufficient for associational standing); *NetChoice, LLC v. Fitch*, 134 F.4th 799, 804 (5th Cir. 2025) (similar).

21. *Second*, in challenging the Act, “the interests at stake are germane to [CCIA’s] purpose.” *Friends of the Earth v. Laidlaw Env’t Servs. (TOC), Inc.*, 528 U.S. 167, 181 (2000); see *Uthmeier*, 2026 WL 3071065, at *4. The Act imposes unconstitutional restrictions on CCIA members’ ability to speak and facilitate speech through app stores and mobile apps. Those constraints directly confront CCIA’s mission to promote open markets, open systems, and open networks, and advocate for the interests of the world’s leading providers of technology products and services.

22. *Third*, CCIA’s members do not need to participate in this suit as parties “for the simple reason that [CCIA] seeks declaratory and injunctive relief, rather than damages.” *Uthmeier*, 2026 WL 3071065, at *6. For example, because the verification and consent requirements affect all covered app stores equally, their claims “can be proven by evidence from representative injured members” like Google, as is the case here. *Fitch*, 134 F.4th at 805 (quoting *Ass’n of Am. Physicians & Surgeons, Inc. v. Texas Med. Bd.*, 627 F.3d 547, 552 (5th Cir. 2010)).

JURISDICTION & VENUE

23. This Court has subject-matter jurisdiction under 28 U.S.C. §§ 1331 and 1343(a). This Court has authority to grant legal and equitable relief under 42 U.S.C. §§ 1983 and 1988, injunctive relief under 28 U.S.C. § 1651 and *Ex parte Young*, 209 U.S. 123 (1908), and declaratory relief under 28 U.S.C. § 2201(a).

24. This Court has personal jurisdiction over Defendant because the Alabama Attorney General resides in and/or conducts a substantial portion of his official business in Montgomery, Alabama.

25. Venue is proper in this district under 28 U.S.C. § 1391(b) because Defendant resides in Alabama, and the events giving rise to this civil action occurred in Montgomery, Alabama.

BACKGROUND & FACTUAL ALLEGATIONS

26. **App Stores Are a Vibrant Forum for Speech.** App stores are digital content services that publish, disseminate, and allow users to search for, browse, discover, download, and purchase mobile apps and other expressive content. In providing this service, app stores facilitate secure, privacy-protective access to vast quantities of expressive content in every digital media format, as well as apps that provide speech and allow users to create, receive, and exchange speech on a vast array of topics. In addition to hosting and disseminating third-party speech, app

stores also exercise judgment over what third-party speech to include and distribute through their services.

27. App stores are teeming with protected speech, as evidenced by the vast number of apps they make available that allow users to create, engage in, and find speech. These apps themselves embody, create, and curate diverse fora for speech and interaction, including a wide range of communication services like WhatsApp, news sources like the Wall Street Journal, search engines like Google, games like Monopoly Go!, social media services like Instagram, and video streaming services like Peacock.

28. App stores further provide access to information, including maps (e.g., Google and Apple Maps), encyclopedias (e.g., Wikipedia), dictionaries and thesauruses (e.g., Merriam-Webster), astronomy charts (e.g., Stellarium), and other reference materials (e.g., Animal Encyclopedia; Audubon Bird Guide). App stores further provide access to smaller developers' educational, skill-building, and cultural apps—including Alabama newspapers, news channels, libraries, and other publishers. The internet is a vital forum for speech, *Packingham*, 582 U.S. at 104, including when it is accessed via mobile devices through apps made available on app stores. Mobile phones, and their capacity to provide access to the speech forums of the internet through mobile applications, have become a leading vehicle for accessing the internet, particularly among younger generations. In short, people use

app stores and the apps they make available “to engage in a wide array of protected First Amendment activity on topics ‘as diverse as human thought.’” *Id.* at 105 (discussing social media users and websites). App stores stand at the threshold of access to that protected activity.

29. App stores embody and facilitate such diverse fora for speech in part because barriers to entry are kept low. Most apps are run by small businesses, and many are run by individual developers. For instance, Apple has noted that 90% of all developers in its App Store are “small developers.”² Thus, apps carry out the internet’s promise of “relatively unlimited, low-cost capacity for communication of all kinds.” *Reno v. ACLU*, 521 U.S. 844, 870 (1997).

30. The vast majority of the most-downloaded apps in member app stores either offer or facilitate content that would unambiguously constitute protected expression, including news, politics, education, video streaming, ebooks, music, games, communication, and information.³ *See 303 Creative LLC v. Elenis*, 600 U.S. 570, 587 (2023); *Brown v. Ent. Merchs. Ass’n*, 564 U.S. 786, 791 (2011); *Sorrell v.*

² *Small developers on the App Store grew revenue by 71 percent over the past two years*, Apple Newsroom (May 11, 2023), <https://www.apple.com/newsroom/2023/05/small-developers-on-the-app-store-grew-revenue-by-71-percent-from-2020-2022/>.

³ *See, e.g., Top Charts*, Google Play, https://play.google.com/store/apps?hl=en_US (last visited Oct. 15, 2026); *Top Charts - Top Free Apps*, Apple App Store, <https://apps.apple.com/us/charts/iphone/top-free-apps/36> (last visited Oct. 15, 2026); *Best Sellers in Apps & Games - Top 100 Free*, Amazon Appstore, https://www.amazon.com/gp/bestsellers/mobile-apps/ref=zg_bs?ie=UTF8&tf=1 (last visited Oct. 15, 2026).

IMS Health Inc., 564 U.S. 552, 570 (2011). Across these categories, apps categorized as “Games,” “Entertainment,” “Social,” and “Communication” comprised approximately 47% of app downloads across the Apple App Store and Google Play in 2025.⁴

31. Examples of the vast array of apps that provide access to fully protected speech and information include:

- a. **Substack**, which allows individual writers to develop a readership and monetize their writing;
- b. **Khan Academy**, which provides educational content to assist people in learning a wide range of subjects;
- c. **Wikipedia**, which allows users to search and explore millions of articles in hundreds of languages;
- d. **The Animal Encyclopedia**, which people can use to observe, learn, and grow their knowledge about more than one hundred animals from around the world;
- e. **Audubon Bird Guide**, which provides a free field guide to over eight hundred species of North American birds;

⁴ *App Downloads by Category in 2025*, AppTweak (Dec. 15, 2025), <https://www.apptweak.com/en/reports/app-downloads-by-category>.

- f. **YouVersion Bible App**, which allows people to read or listen to the Bible and share passages and comments with friends in their network;
- g. **InstaRabbi**, which allows Jews from across the world to ask Torah or Halachic questions and get quick answers in accordance with Orthodox Jewish observance;
- h. **Merriam-Webster Dictionary**, which gives access to one of the most used and respected English-language dictionaries in the United States, providing readers with hundreds of thousands of definitions;
- i. **Spotify**, which allows people to listen to music, podcasts, and audiobooks and share playlists with others;
- j. **NYTimes** and **WSJ Print Edition**, which provide journalism, just as they do in their print newspapers;
- k. **AL.com**, which gives readers access to trusted local news across Alabama, including breaking news and in-depth reporting;
- l. **The Alabama Crimson Tide mobile app**, which lets fans of the Alabama Crimson Tide view exclusive content and access scores and stats around Alabama games;
- m. **Tankee**, a gaming and video sharing service that curates family-friendly content and helps parents ensure that their kids are not watching adult-oriented videos;

- n. **Gabb Messenger**, an app made specifically to protect kids, connect families, and empower parents that allows friends and family to safely video call and message with kids using Gabb directly through the app;
- o. **Waffle Smash**, a family-friendly game that allows kids to put their skills to the test and tackle fun, challenging puzzles;
- p. **StoryPlace**, an online community that allows writers to share original stories;
- q. **Smart Kidz Club**, an educational service that helps foster kids' love of reading and math;
- r. **Sudoku Master®**, which allows people to choose from tens of thousands of Sudoku puzzles to play.

32. CCIA's members own and operate dozens of speech-facilitating and speech-creating apps, including Apple TV, Apple Games, YouTube, Gmail, Goodreads, Kindle, Audible, and IMDb. These apps, and numerous others, provide users with access to a vast array of protected speech, including books, movies, videos, music, reviews, and factual information, as well as the ability to create and share their own speech in various forms.

33. In addition to their content, apps embody expressive software design choices, and their operation and maintenance constitute speech acts.

34. Apps improve the user interface of websites on phones and tablets. But users can often access the same material available in a mobile app via other means, including web browsers (which, when used on mobile devices, are apps themselves) and non-mobile apps. For example, a user can stream music on Spotify or read essays on Substack through their mobile apps but can also access the same content through their websites via web browsers on mobile devices or computers. Likewise, Amazon Prime Video and YouTube are available through their respective mobile apps, but also through their respective websites ([primevideo.com](https://www.primevideo.com) and [youtube.com](https://www.youtube.com)) or through non-mobile apps that can be downloaded on a Smart TV. The Act's impact is thus to segregate content available through apps behind age-based restrictions while doing nothing to prevent access to the exact same material through other means, making accessing speech and information more difficult and disjointed.

35. **App Stores and Apps Already Have Policies and Voluntary Tools to Help Protect Minors from Inappropriate Speech.** App stores facilitate the vast majority of app downloads by mobile device users. App stores curate and review the apps they offer for download, both prior to and after publication, to provide quality controls and additional services for users based on industry standards. For example, CCIA's app store members all require app developers to submit to a rigorous pre-publication review process, wherein the app store will evaluate the app's content, check the security of the app, and test its functionalities in an isolated environment.

Part of this process involves rating the app's content to determine its age-appropriateness.

36. Further, CCIA's app store members all engage in age-rating, but each app store has a different age-rating system and different age categories. These processes and categories, which are based on or exceed global industry standards, differ from the age categories imposed by the Act. The Google Play Store, for example, uses a separate rating authority, the International Age Rating Coalition, which screens apps and assigns them each a rating based on Entertainment Software Rating Board ("ESRB") guidelines.⁵ Apple's App Store similarly requires age rating for "parental controls" and uses categories 4+, 9+, 13+, 16+, and 18+. ⁶ The Apple App Store employs even more granular age-rating categories for apps designated in its "Kids Category," placing apps in one of three age bands based on its primary audience: "5 and under, 6 [to] 8, or 9 [to] 11."⁷

37. CCIA's app store members also review apps in accordance with their content policies and block or remove from their stores those that they consider harmful, low quality, unsafe, or otherwise inconsistent with their content policies.

⁵ *Requirements related to content ratings for apps, games, and the ads served on both*, Google Play, <https://support.google.com/googleplay/android-developer/answer/9859655> (last visited Oct. 15, 2026).

⁶ *Age ratings values and definitions*, Apple Developer, <https://developer.apple.com/help/app-store-connect/reference/age-ratings-values-and-definitions/> (last visited Oct. 15, 2026).

⁷ *Design safe and age-appropriate experiences for your apps and games*, Apple Developer, <https://developer.apple.com/kids/> (last visited Oct. 15, 2026).

For example, the Google Play Store prohibits apps “that contain or promote sexual content or profanity,” including “pornography and content or services intended to be sexually gratifying or to solicit sexual acts for compensation.”⁸ Amazon and Apple have similar policies.⁹

38. For apps directed toward younger audiences, CCIA’s app store members also impose and enforce even stricter content policies. Those apps generally must contain only age-appropriate content, implement parental consent gates for purchasing opportunities, and protect against disclosure of children’s personal information, among other requirements.

39. CCIA’s app store members also provide ongoing monitoring and enforcement of their published content policies. Member app stores monitor apps for compliance both pre-publication and post-publication, and will suspend, reject, or bar apps that do not abide by their policies.

40. On top of these app store monitoring and oversight activities, CCIA’s app store members also provide voluntary tools for parents to control their children’s exposure to apps and the content they contain. The Google Play Store allows parents

⁸ *Inappropriate Content*, Google Play Console Help, <https://support.google.com/googleplay/android-developer/answer/9878810?hl=en> (last visited Oct. 15, 2026)

⁹ *Amazon AppStore Content Policy*, Amazon Developer, <https://developer.amazon.com/docs/policy-center/understanding-content-policy.html> (last visited Oct. 15, 2026); *App Review Guidelines*, Apple Developer, <https://developer.apple.com/app-store/review/guidelines/> (last visited Oct. 15, 2026).

to set up controls on their children's accounts.¹⁰ These controls allow parents to, for example, restrict apps and games on an Android device by choosing categories of content allowed for download or purchase; lock their child's screen during certain hours such as bedtime; approve all purchases and new apps that the child wants to download; and more.¹¹ The Apple App Store similarly allows parents to set age-related restrictions for content, prevent their children from installing and purchasing apps, set restrictions for Siri and Game Center, set screentime schedules, and manage their child's privacy settings.¹² Additionally, Amazon's Parent Dashboard allows parents to monitor the apps their children are interacting with, set daily limits or restrict their children's use at certain times of day, and restrict access to content that parents might find inappropriate for their child.¹³ These parental controls are popular: The Google Family Link app has over 100 million downloads in the Google Play Store alone, and the Amazon Parent Dashboard has over 1 million downloads in the Google Play Store.

41. By crafting, publishing, and enforcing content policies and providing tools to allow parents to limit access to app content, app stores actively engage in

¹⁰ *How to Set Up Parental Controls on Google Play*, Google Play, <https://support.google.com/googleplay/answer/1075738?hl=en> (last visited Oct. 15, 2026).

¹¹ *Id.*

¹² *Use Parental Controls on Your Child's iPhone or iPad*, Apple, <https://support.apple.com/en-us/105121> (last visited Oct. 15, 2026).

¹³ *Amazon Parent Dashboard*, Amazon.com, <https://www.amazon.com/parentdashboard/intro> (last visited Oct. 15, 2026).

expressive activities, selecting which apps to publish, to whom, when, and how. For much the same reason that bookstores receive First Amendment protection for distributing books, app stores receive protection for distributing mobile apps. *See Smith v. California*, 361 U.S. 147, 150 (1959) (“publication and dissemination of books and other forms of the printed word furnish very familiar applications of these constitutionally protected freedoms”).

42. Implementing the State’s mandated age verification, parental-identity verification, parental-tethering, and parental-consent processes will require significant and unrecoverable resources—even for large app stores. And for the numerous small developers in particular, the costs of complying with the Act’s requirements, paired with the threat of liability for failure to comply properly, might disincentivize those small developers from developing new apps or publishing speech through app stores. These costs are particularly unreasonable given that parents already have widely available tools to monitor and control what their children access online. All of CCIA’s member app stores already permit parents to monitor content, restrict downloads, and disable in-app purchases.

ALABAMA ACT NO. 2026-59: RELEVANT PROVISIONS

43. **Age Verification, Parental Tethering, and Parental-Identity Verification to Enable Parental Consent (“Account Restrictions”).** Under the Act, whenever an individual creates an account with an app store, the app store must

“[v]erify the individual’s age category using” either “[c]ommercially available methods that are reasonably designed to ensure accuracy,” or “[a]n age verification system that complies with rules adopted pursuant to this act.” § 2(a)(2). A method is “commercially available” if it includes both (1) “affirmative age attestation by an individual who is reasonably believed to be the parent or legal guardian of the minor” and (2) “other information collected in the ordinary course of account creation or use.” § 2(b). “Age category” is a term of art under the Act, and sorts individuals into four groups: younger than 13; at least 13 and younger than 16; at least 16 and younger than 18; and at least 18. § 1(2).

44. If the user is determined to be under 18, the Act requires the account to be affiliated with a “parent account.” §§ 1(16), 3(1). The “parent” must be a biological parent, legal guardian, or individual with legal custody of the minor. § 1(15). In addition, the app store is required to verify that the parent is not a minor. §§ 1(16), (20).

45. App developers are required to “[r]equest age category data or verifiable parental consent” whenever an account holder downloads or purchases an application or launches a pre-installed app for the first time, or whenever the developer implements a “significant change” to the app. § 9(a)(4). Developers must verify the age category assigned to each user in Alabama and, for minors, whether parental consent has been obtained, based on information provided by the app store.

§ 9(a)(1). Developers must limit use of that data to “enforce developer-created age-related restrictions, protections, or defaults,” “ensure compliance with applicable laws or regulations,” and “implement safety-related features or defaults.” § 9(a)(3). However, the Act *also* provides that developers must “use the lowest age category indicated by” either the age category data provided by the app store *or age data independently collected by the developer* when implementing safety-related features or defaults. § 9(a)(5).

46. The Act does not provide any guidance on how to determine whether an adult has a parental status with respect to the minor sufficient to be affiliated.

47. The choice of using either “[c]ommercially available methods that are reasonably designed to ensure accuracy” or “an age verification system that complies with rules adopted pursuant to this act” does not alter which app stores or apps the Act covers. § 2(a). Nor does the purported availability of alternative methods of compliance alleviate the unconstitutional burdens or diminish the chilling effect that age- and legal authority-verification imposes on users’ access to protected speech.

48. **Parental Consent Requirement for Each App Downloaded (“Download Restrictions”).** In addition to age verification, app stores must obtain consent from the parent account each time a minor seeks to download or purchase an app or make an in-app purchase. § 3(2). The statute has no provision that would

permit parents to opt out of or streamline this onerous consent requirement. And because verifiable parental consent requires providing a disclosure that includes information *about the specific app being consented to*, § 1(17), the Act makes blanket consent to all apps impossible in practice.

49. **Ongoing Parental-Consent Requirement for In-App Purchases and Significant Changes to App Terms (“Purchase and Renewed Access Restrictions”).** App stores must also obtain verifiable parental consent on an ongoing basis *every single time* a minor wants to make an in-app purchase. § 3(2)(iii). Further, the Act requires app developers to provide notice to app stores upon making any so-called “significant change” to the app’s terms of service or privacy policy, vaguely defined as a change that, for example, alters the age rating assigned to the app or “adds new monetization features, including, but not limited to, in-app purchases or advertisements, where no such features were previously present.” §§ 1(19), 9(a)(2). When such a change is made, the Act also requires app stores to notify any individual who gave consent for a minor’s download or purchase relating to a previous version of the changed app and to obtain consent for minors’ continued use or purchase of the app. § 4(1)–(2).

50. **Age Rating, Content Description, and Disclosure Requirements.** The Act could also, but should not, be read to effectively compel app developers and app stores to engage in subjective and potentially controversial speech through its

vague age rating and disclosure requirements. Specifically, the Act requires the app store to disclose an app’s or in-app purchase’s age rating or content description, if one is available, in order to obtain “verifiable parental consent.” § 1(17), (20). The Act also holds both developers and app stores liable for “knowingly misrepresent[ing]” any information in that disclosure. §§ 8(2), 9(c)(2). At the same time, a developer is protected by a safe harbor from the risk of liability for this “knowing[] misrepresent[ation]” provision if the developer “uses widely adopted industry standards to determine” the “age category”—a term defined in the Act to refer to specific age ratings provided by the Act—and the “content description”—meaning the specific content elements or functions that inform the app’s age rating. §§ 1(2), 1(8), 12(b). Similarly, developers are required to request age verification data collected by app stores *using the State’s age categories*, § 9(a)(1), and simultaneously required to limit the use of this data to “enforce developer-created age-related restrictions, protections, or defaults,” “implement safety-related features or defaults,” and “ensure compliance with applicable laws or regulations.” § 9(a)(3).

51. These provisions might be read to require that, in order to avoid liability under the Act, developers must implement an elaborate, vaguely-defined age-rating system according to the Act’s specified age categories and provide those ratings and a content description justifying those ratings to app stores, and that app stores must blindly parrot those age ratings for apps and in-app purchases to minor users’ parents

“clearly and conspicuously,” regardless of their own judgment regarding age-appropriate designations. § 1(20). The lack of clarity regarding whether this is the proper interpretation of the Act illustrates the Act’s vagueness.

52. Developers must also notify app store providers of significant changes to their apps, defined to include “a material modification to an app’s terms of service or privacy policy” that alters the app’s age rating or content descriptions or adds new monetization features (including in-app purchases or advertisements). § 1(19).

EFFECTS OF ACT 2026-59’S VERIFICATION AND CONSENT REQUIREMENTS

53. The verification and consent requirements violate app stores’, developers’, and users’ First Amendment rights to publish, disseminate, provide access to, and curate protected speech. App stores enjoy First Amendment protection both when they publish and disseminate speech, *e.g.*, *Sorrell*, 564 U.S. at 557, and when they “present[] a curated compilation of speech originally created by others.” *Moody v. NetChoice, LLC*, 603 U.S. 707, 728 (2024). Apps themselves—including, for example, books, movies, and games—are expressive, embodying expressive design decisions and providing access to a wealth of speech, information, ideas, and expression.

54. The verification and consent requirements impose direct burdens on app stores’ freedom to disseminate protected speech. At the threshold, the age-verification requirement inserts a barrier between speech disseminated through the

app stores and the audience of that speech—blocking many users entirely. Subsequently, even for users who comply with this initial gatekeeping mechanism, minor users will be unable to access any speech whatsoever until they complete the further parental verification and consent steps. Unless and until a user either proves they are at least 18 years old, or a verified parent or guardian takes affirmative steps to permit their child to access apps for download or purchase, the Act prohibits app stores from disseminating protected speech to those users.

55. The verification and consent requirements similarly burden the First Amendment rights of app developers, by imposing a “parental veto” between users’ ability to access, download, and purchase developers’ speech. *See Brown*, 564 U.S. at 795 n.3. The Act imposes a blanket ban on anyone under 18 downloading any app or purchasing any in-app content without parental consent. For example, a 17-year-old cannot download the “Wall Street Journal News” app until his parent or guardian provides consent for the download. Nor will he be able to open the pre-installed “Apple Games” app on his iPhone. Similarly, a 14-year-old cannot purchase the audiobook version of *The Giver* from Audible until her parent or guardian approves the purchase. If the minors’ parents or guardians are too busy, or refuse to approve the request, or cannot adequately prove their identities, the minors would be blocked entirely from reading breaking news reported by the Wall Street Journal or listening to the John Newbery Medal-winning novel. This gatekeeping mechanism

simultaneously deprives the minor user of his or her right to access protected speech *and* prevents app developers from disseminating their speech to interested audiences.

56. The verification and consent requirements also burden users of mobile apps. Both app stores and app developers can assert the First Amendment rights of their users. *See, e.g., Broadrick v. Oklahoma*, 413 U.S. 601, 612 (1973); *Brown*, 564 U.S. at 794-96. Although the Act is purportedly about protecting children, age verification places all protected speech on app stores behind a wall and thus burdens the rights and interests of *all* app store users, including adults. Everyone who creates an account—essentially everyone with a mobile phone—is required to have their age verified and to submit sensitive, personal documentation or biometric information before they will be allowed to access protected speech.

57. Age verification burdens users' ability to speak and access speech. Verification methods generally ask users to upload a government-issued ID, such as a driver's license or passport, or input credit card information. This will, at best, deter users (many of whom do not wish to disclose this type of sensitive information to app stores) from accessing the tremendous amount of expressive and informational offerings within the app stores and from engaging in the protected speech and knowledge-seeking they facilitate. At worst, these methods will carve out substantial segments of the population from being able to comply at all. For

instance, about 15 million adult U.S. citizens do not have a driver’s license, while about 2.6 million do not have any form of government-issued photo ID.¹⁴ Further, the Federal Reserve reports that, in 2023, approximately 18% of adults in the United States did not have a credit card.¹⁵ Additionally, “[c]hildren generally don’t have government IDs[,]”¹⁶ and often do not have credit cards, either.¹⁷

58. Mandated verification also prioritizes the State’s goals and subordinates users’ privacy preferences. Currently, there is no technically feasible and reliable way to verify the ages or age categories of online users at account creation without processing personally identifiable information that many do not want to share.¹⁸ All age-verification methods also risk excluding some members of

¹⁴ Jillian Andres Rothschild et al., *Who Lacks ID in America Today? An Exploration of Voter ID Access, Barriers, and Knowledge*, Univ. Md. Ctr. for Democracy & Civic Engagement, at 2 (Jan. 2024), <https://cdce.umd.edu/sites/cdce.umd.edu/files/pubs/Voter%20ID%202023%20survey%20Key%20Results%20Jan%202024%20%281%29.pdf>.

¹⁵ Report on the Economic Well-Being of U.S. Households in 2023, U.S. Federal Reserve (May 2024), <https://www.federalreserve.gov/publications/files/2023-report-economic-well-being-us-households-202405.pdf>.

¹⁶ Shoshana Weissmann, *Kids Don’t Have IDs and Age-Estimation Tech Is Frequently Very Wrong*, Techdirt (May 23, 2025), <https://www.techdirt.com/2025/05/23/kids-dont-have-ids-and-age-estimation-tech-is-frequently-very-wrong/>.

¹⁷ See Dawn Papandrea, *46% of Parents Say Their Child Used Their Credit or Debit Card Without Permission, Racking Up \$500+*, LendingTree (Mar. 1, 2022), <https://www.lendingtree.com/credit-cards/study/kids-and-credit-cards-survey/> (“Overall, 22% of parents say their minor child is an authorized user.”).

¹⁸ See Trevor Wagener, *App Store Age Verification: Popular in Principle, Unworkable in Practice*, CCIA (Oct. 21, 2025), <https://ccianet.org/articles/app-store-age-verification-popular-in-principle-unworkable-in-practice/> (“In a nationally fielded survey, two-thirds of Americans said they are not comfortable sharing their own government ID with social media companies to verify age, and 70% are not comfortable sharing their child’s ID.”).

the population, e.g., those without government IDs and those who wish to use mobile app stores and apps anonymously, without disclosing data to app stores.

59. Yet the Act imposes far greater privacy invasions than a traditional age verification law. Beyond merely gating access to a narrow category of age-sensitive material (like alcohol or pornography), the Act's all-encompassing sweep virtually guarantees that all smartphone users in Alabama will have to submit to age verification to download a single app from an app store. And unlike most other age-verification laws, the Act requires a minor's account to be affiliated with a separately verified parent account. This unique second step necessarily requires the app store to double its collection of highly sensitive personal information to ensure that the purported parent is in fact the minor's biological parent, legal guardian, or individual with legal custody. § 1(15).

60. These verification requirements then feed into the Act's unnecessarily onerous parental consent requirement every time a minor wants to download or purchase almost any mobile app, make an in-app purchase, or continue to use an app after its terms of use or privacy policy have been "significant[ly]" changed. This means that minors are effectively prohibited from accessing protected speech unless and until their parent or legal guardian can be verified by the app store and then, on an app-by-app and purchase-by-purchase basis, grant access. This requirement will

impose real friction on minors’ abilities to access constitutionally protected content, even where their parents would not otherwise object.

61. Beyond the direct burdens on users’ access to speech and personal privacy interests, the Act’s verification and consent requirements also impose immense practical and financial burdens on app stores, which in turn further burden developers and users in accessing and participating in the stores. For instance, app stores must provide developers with a user’s age category and consent status in order to perform their own verifications. That requires app stores to expose millions of users’ age categories to millions of developers regardless of whether a user or parent has consented to that sharing, and regardless of whether a developer can securely handle such large amounts of sensitive information. § 5. The burdens associated with developing the new systems mandated by the Act, plus the privacy infringements inherent to verification and the frictions imposed by the constant need to provide consent, will ultimately decrease the diversity and the totality of speech available to all people, particularly minors—but also adults.

62. Parental identity verification poses additional practical hurdles that will bar large swaths of developers from disseminating—and huge numbers of users from accessing—lawful speech. The Act provides no guidance on how app stores should ensure that a “parent” seeking affiliation with a minor’s account is in fact a “parent” as defined by the law. Parents often have different last names than their children and

may have a different address; most children do not have government IDs; parents who are estranged from each other may have opposing views about what their children can and cannot have access to; children who have been emancipated may not have the necessary “parent” to comply with the Act, and may be unable or unwilling to provide documentation establishing their emancipated status; and children in foster care or who are orphaned may not have a legal guardian who is able or willing to link their mobile device to the child’s account. Nor does the Act appear to consider the complexities that could arise where, for example, a parent and child have mobile phones or tablets with different operating systems and, as a result, different app stores.

63. Minors who are unable to link their device with a parent or guardian will be effectively barred from one of the most important and ubiquitous modern forums for accessing and engaging in protected speech. And even minors who are successful in linking their account with a parent or guardian will still be significantly burdened in exercising their First Amendment rights because they will be forced to wait for parental consent in order to purchase individual publications or other expressive content to read, listen to, or watch.

64. These added difficulties are entirely superfluous to—and in fact undermine—any interest that Alabama may have in empowering parents. The Act mandates conduct that app stores and many individual app developers *already*

undertake, namely, providing parental controls that allow parents to monitor and control what their children can access on their devices. Again, by *legally requiring* parental consent—even for parents who prefer to give their children autonomy and even for minors on the brink of adulthood—the Act imposes the State’s authority, not parents’, over the children of Alabama.

65. The operational hurdle created by the need to obtain consent for every app download, purchase, in-app purchase, and “significant change” to an app’s privacy policy or terms of service will be endlessly frustrating for parents and their children. Under the Act, app stores are in practice prohibited from allowing parents to provide blanket consent for their children to download or purchase apps or make in-app purchases. §§ 1(17), 3(2). This hurdle is yet another indication that, rather than providing parents with oversight of their children, the law imposes *the State’s control* over what Alabama children may access, “subject only to a parental veto.” *NetChoice, LLC v. Griffin*, No. 5:23-CV-5105, 2025 WL 978607, at *10 (W.D. Ark. Mar. 31, 2025) (cleaned up) (quoting *Brown*, 564 U.S. at 795 n.3, 804), *appeal filed*, No. 25-1889 (May 2, 2025). The constant inundation with consent requests also runs the risk of “consent fatigue”—parents will stop paying attention to them and simply approve the request, further undermining the purpose of the Act. Moreover, these requirements will disincentivize developers from making appropriate updates to

their privacy policies and terms of use to avoid triggering the Act’s renewed parental consent obligation.

66. The Act’s failure to accommodate or account for existing and robust parental controls and its failure to provide parents with any choice in how they supervise their children underscore the Act’s overbreadth and lack of narrow tailoring. *Cf. Uthmeier*, 2026 WL 3071065, at *14 (upholding law with “numerous limitations” including that it does not apply to all platforms). By contrast, a law that allowed parents to make use of the extensive tools already available, or at the least to streamline or categorize their consent, would ensure a more tailored and appropriate fit between means and ends. This would allow parents to decide for themselves how to oversee their children’s online activity, and would allow app developers the discretion to tailor their requirements according to the rigor called for by the unique content of the app.

EFFECTS OF THE ACT’S AGE-RATING AND DISCLOSURE REQUIREMENTS

67. The Act’s age-rating provisions could, but should not, be read to impermissibly seek to compel app developers to create and disclose opinions about the content of their apps and any third-party content offered for purchase within their apps. Similarly, the age-rating disclosure requirement could be read to compel app stores to communicate controversial third-party opinions about the content of the apps they disseminate. To the extent these are the proper interpretations of these

provisions, both provisions infringe on app developers’ and app stores’ right to free expression and “offend[] the First Amendment.” *303 Creative*, 600 U.S. at 586–87.

68. The Act requires both app stores and developers to identify users’ ages within four categories: under 13 years of age; at least 13 years of age but less than 16; at least 16 years of age but less than 18; or at least 18 years of age. § 1(2). The gradations between each of these categories require relatively high degrees of specificity, and the success of the Act is in large part dependent on accurate categorization (within the State’s judgment of accuracy). Nor do these categories track the age buckets used by many leading app stores, and the Act provides no criteria for determining what constitutes a sufficiently “widely adopted” industry standard or for determining, for example, what type of app would be appropriate for a group of 13- to 15-year-olds versus 16- and 17-year-olds.

69. The Act also could be read to, in practice, force developers to rate their apps and in-app purchases along those four arbitrary age buckets in order to avoid liability. Developers may be liable under the Act for knowingly misrepresenting the age rating of a given app or in-app purchase. § 9(c)(2). And if an age rating for an app or in-app purchase is “available” to an app store, it must be included in the parental consent disclosure. § 1(17). A developer is protected from liability for knowingly misrepresenting the age rating of an app if the developer “uses widely adopted industry standards to determine the app’s age category.” § 12(b). The term

“age category” specifically means *Alabama’s chosen age ratings*. § 1(2). Thus, in order to take advantage of the Act’s safe harbor and avoid liability for any misrepresentations related to the age rating in a parental disclosure, developers are in practice required to adopt the Act’s age categories and then provide those categories (and content descriptions that justify them) to app stores. Further bolstering this requirement, the Act obligates developers to verify through app stores *the State’s age categories* for every user in Alabama, § 9(a)(1), and instructs that developers shall limit their use of the age category data they receive to: “ensur[ing] compliance with applicable laws or regulations,” “enforc[ing] developer-created age-related restrictions, protections, or defaults,” “implement[ing] safety-related features or defaults,” such as age ratings for in-app purchases, § 9(a)(3).

70. When app developers, as described above, are in practice forced to set age ratings for their apps that align with the Act’s age categories and provide those ratings and content descriptions justifying their rating decisions to app stores, app stores will be compelled to disclose those ratings and descriptions to parents every time a minor wants to download or purchase an app or make an in-app purchase, and every time a developer makes a change that alters the app’s age rating or content descriptions. §§ 3(2), 4.

71. Age ratings in similar contexts (e.g., library materials and video games) are notoriously subjective, imperfect, and open to different interpretations. *See, e.g.,*

Book People, Inc. v. Wong, 91 F.4th 318, 329–30 & n.49 (5th Cir. 2024); *Ent. Software Ass’n v. Blagojevich*, 469 F.3d 641, 651–52 (7th Cir. 2006); *Video Software Dealers Ass’n v. Schwarzenegger*, 556 F.3d 950, 966–67 (9th Cir. 2009) (“Unless the Act can clearly and legally characterize a video game as ‘violent’ and not subject to First Amendment protections, the ‘18’ sticker does not convey factual information.”), *aff’d sub nom.*, *Brown v. Ent. Merchs. Ass’n.*, 564 U.S. 786 (2011).

72. These age-rating, content description, and disclosure requirements will encourage app developers to self-censor, as they will be incentivized to appeal to the largest possible audience and thus to avoid ratings that may discourage users from downloading (or consenting to their children downloading) the app. They will deter developers from making “significant changes” to the terms of service or privacy policy when those alterations would affect the app’s age rating and thus trigger the requirements to notify app stores and obtain renewed consent. And for apps that host third-party content, developers may be more inclined to engage in content-moderation practices designed to facilitate particular, pre-determined age ratings, as opposed to the app’s independent editorial judgment about its own content guidelines.

CLAIMS

73. CCIA raises the following claims:

- a. **Count I:** a First Amendment challenge to the verification and consent requirements and their associated violation provisions, brought as-applied with respect to the provisions affecting CCIA's member app stores (Google, Apple, and Amazon);
- b. **Count II:** a First Amendment challenge to the verification and consent requirements and their associated violation provisions, brought facially with respect to the provisions affecting app stores;
- c. **Count III:** a First Amendment challenge to the verification and consent requirements and their associated violation provisions, brought as-applied with respect to the provisions affecting CCIA's developer members, including YouTube, Audible, IMDb, Twitch, and Gmail, among others;
- d. **Count IV:** a constitutional challenge to the age-rating, content description, and disclosure requirements and associated violation provisions brought as-applied to CCIA members in their capacities as developers, including YouTube, Audible, IMDb, Twitch, and Gmail, among others;

- e. **Count V:** a vagueness challenge to the age-rating, content description, and disclosure requirements and associated violation provisions;
- f. **Count VI:** a vagueness challenge to the notice of significant changes provision;
- g. **Count VII:** a Commerce Clause challenge as to the Act as a whole; and
- h. **Counts VIII & IX:** requests for equitable and declaratory relief related to the above claims.

74. A challenge is as-applied “[w]here plaintiffs challenge the validity of a statute because they seek to vindicate their own rights.” *DA Mortg., Inc. v. City of Miami Beach*, 486 F.3d 1254, 1262 (11th Cir. 2007). CCIA’s as-applied First Amendment challenges are brought as to its app store members, Google, Apple, and Amazon, and as to its developer members, including the developers of YouTube, Audible, IMDb, Twitch, and Gmail (among others). As-applied to each of these members, the Act’s verification and consent regime creates barriers to, and in some cases fully blocks, users’ ability to access both CCIA’s members’ app stores and CCIA’s developer members’ apps, thus violating the First Amendment.

75. For the First Amendment claims, the facial challenge standard asks whether “a substantial number of [the Act’s] applications are unconstitutional, judged in relation to the statute’s plainly legitimate sweep.” *Moody*, 603 U.S. at 723 (citation omitted). The Act has *no* constitutional applications to app stores. The Act’s

main verification and consent provisions, “in every application to a covered [app store], raise the same First Amendment issues,” so the Court “need not ‘speculate about “hypothetical” or “imaginary” cases.’” *X Corp. v. Bonta*, 116 F.4th 888, 899 (9th Cir. 2024) (quoting *Wash. State Grange v. Wash. State Republican Party*, 552 U.S. 442, 450 (2008)). Indeed, the Act’s threshold verification and consent requirement has but a single application to each app store, which applies uniformly and broadly: every person who wishes to create an account on an app store must submit to age verification, and every person under 18 must obtain parental consent before the account can be created and even a single app can be accessed through the app store. The Act’s indiscriminate barriers to access impose burdens that fall uniformly across all app stores whose speech can no longer be freely accessed. And they also apply uniformly to all users, whose access to protected speech is burdened or entirely foreclosed.

76. For CCIA’s First and Fourteenth Amendment vagueness claims, a facial vagueness challenge is proper because “there is no reason to believe one [app developer] is better suited than another to understand [the Act’s] vague terms.” *CCIA v. Paxton*, 747 F. Supp. 3d 1011, 1031 (W.D. Tex. 2024); *see also CCIA v. Paxton*, 814 F. Supp. 3d 787, 802–03 (W.D. Tex. 2025) (finding facial challenge appropriate and invalidating nearly identical app store law’s “notice of any significant change[s]” provision as unconstitutionally vague).

77. Each First and Fourteenth Amendment challenge raises the rights of both CCIA members and those who use or could prospectively use CCIA members' app stores or apps.

COUNT I
42 U.S.C. § 1983; Ex Parte Young
VIOLATION OF THE FIRST AMENDMENT, AS INCORPORATED
AGAINST THE STATES THROUGH THE FOURTEENTH AMENDMENT
(Verification and parental-consent requirements as-applied to app stores,
Alabama Act No. 2026-59 §§ 1–8)

78. CCIA incorporates all prior paragraphs as if fully set forth herein.

79. **The Act Burdens Dissemination of, Curation of, and Access to Protected Speech.** The Act is unconstitutional as applied to CCIA's member app stores: the Google Play Store, the Apple App Store, and the Amazon Appstore. At the threshold, it requires these app stores to verify the age of every user before they will be permitted access to their services. It thus broadly bars all Alabamians' access to speech by requiring that they undergo an age investigation process before they can access the myriad protected speech made available on the CCIA members' app stores. The Act then forces any minor user to tether their account to a verified parent or guardian, and before the minor user can download or purchase any app, obtain consent from the verified parent or guardian. These provisions burden the CCIA member app stores', along with app developers' and users', rights to free expression under the First Amendment. Because the Act was passed for content-based reasons,

it triggers and fails strict scrutiny. At minimum, the Act triggers and fails intermediate scrutiny.

80. Countless apps available on CCIA members' app stores provide constitutionally protected speech to both adults and minors, as well as opportunities for app users to create and disseminate their own pure speech. The CCIA members' app stores disseminate this speech, publishing a huge variety of software apps for users to browse and securely download and helping to facilitate access to the speech and other expressive content within or through those apps. In addition, the app stores present a curated compilation of speech originally created by others. The Act's age verification provisions age-gate the primary gateway to the internet on mobile devices and, paired with the consent requirements, unequivocally regulate and burden speech. The gates open only if the individual first passes the app store's age-verification, meaning *all Alabamians* are barred from accessing the internet via the Google Play Store, the Apple App Store, or the Amazon Appstore unless they agree to the Act's invasive verification procedures and, if the user is a minor, the parental-identity verification, parental-tethering, and parental-consent requirements imposed by the Act.

81. For people who do not have documentation necessary to age verify, such as an ID or credit card, they are blocked entirely from receiving and producing speech on every app made available on these app stores. Verification requirements

also create risks of exposing users’ sensitive personal information, and chill speech by depriving users of anonymity they would otherwise be entitled to in connection with the many apps that permit a logged-out experience.

82. Minors must jump through further onerous hoops imposed by the Act. First, a parent account must be linked to the minor account and verify that the individual is a “parent.” §§ 1(15)–(16), 3(1). Then, of course, the parent must decide whether to authorize the minor’s download or purchase of the app. § 3(2). Finally, on an ongoing basis, parents must give further consent every time a minor wants to purchase any item through the app (for example, an audiobook purchased through Audible), *id.*, and every time the app makes a so-called “significant change” to its terms of service or privacy policy, § 4(1)–(2). This burdens minors’ speech by depriving them of their ability to speak and access speech without express parental consent. *Brown*, 564 U.S. at 804–05 (First Amendment principles apply “[e]ven where the protection of children is the object[.]”).

83. **The Act Is Subject to Strict Scrutiny.** The legislative record makes clear that the Act has a content-based justification. Specifically, Alabama seeks to protect minors from exposure to allegedly harmful content made available through app stores. The bill’s sponsor in the House of Representatives, for example, noted in his opening remarks that “[a]pp stores are a gateway to what our children are exposed to online.” *Debate on H.B. 161 Before the Ala. House of Rep.*, 2026 Reg.

Sess. at 27:21–25. Senator Chambliss, describing the Act in the Senate, similarly explained that it shields children from “certain physical information ... until they are mature enough to handle [it].” *Debate on H.B. 161 Before the Ala. Senate*, 2026 Reg. Sess. at 42:32–43 (Feb. 5, 2026), <https://alabamachannel.ompnetwork.org/embed/full/sessions/1280?embedInPoint=0&embedOutPoint=0&shareMethod=link>. The legislative record makes clear that the Act’s purpose is to target specific content made available to minor users on app stores.

84. Perhaps seeking to avoid strict scrutiny (despite the Act’s expressly content-based justification), Alabama broadly drafted the law to target the entirety of speech on CCIA’s member app stores. But Alabama cannot restrict “an entire medium of expression” in the name of evading First Amendment scrutiny. *City of Ladue*, 512 U.S. at 55. In doing so, Alabama has widened the Act’s aperture to “suppress too much speech,” without leaving “adequate substitutes for the important medium of expression” that app stores offer. *Id.* at 55-56.

85. The Act also impermissibly enlists the CCIA members’ app stores to carry out a vast censorship scheme on behalf of the State. *First*, the app stores are forced to verify the age of every single user via invasive age verification procedures at the threshold, before allowing adults 18 and older access to a vast array of protected speech. *Second*, if the user is determined to be a minor, the Act forces

CCIA’s member app stores to deny minors access to speech, “subject only to a parental veto,” *Brown*, 564 U.S. at 795 n.3, by requiring parental consent before a minor may download any app. *Third*, app stores are forced to bar access without parental consent whenever a minor wants to make an in-app purchase or after a developer makes a “significant change” to the app. The Act forces the app stores to impose these restrictions, which will deter adults and minors alike from accessing apps they otherwise would.

86. Even if Strict Scrutiny Did Not Apply, the Verification and Consent Requirements Fail Intermediate Scrutiny. The Act *at minimum* is subject to intermediate scrutiny. *See Uthmeier*, 2026 WL 3071065, at *9. And even under intermediate scrutiny, Alabama could not satisfy its burden. The Act is overbroad in capturing nearly every app within an app store; it fails to account for less restrictive alternatives such as existing voluntary parental tools and more targeted laws such as Alabama Code § 8-19G-3; and it is simultaneously underinclusive by failing to impose any gates around web-based or non-mobile analogs. It also makes no attempt to exempt apps that are irrelevant to the State’s cognizable interest, as evidenced by its practical prohibition on parents deciding to provide blanket consent to their children.

87. The Verification and Consent Requirements Are Overbroad. The Act imposes age-verification as a gate that bars every single Alabamian at the

threshold from accessing any app within an app store, including the vast swaths of protected speech disseminated through apps dedicated to publishing news, fostering creativity, encouraging religious exploration, and providing entertainment and educational resources. With respect to minor users, the Act piles on further burdens via the parental-identity verification, parental-tethering, and parental-consent requirements.

88. The Act makes no attempt whatsoever to link the State's purported interest in protecting minors to the sweeping parental control mandates it imposes.

89. The State's practical prohibition of blanket parental consent underscores the tailoring problem and unnecessarily burdens parents. As written, the Act requires CCIA's member app stores and parents to wade through several layers of consent on an app-by-app and purchase-by-purchase basis. In no world does depriving parents of the opportunity to opt out of the Act's mandatory account restrictions, download restrictions, purchase and renewed access restrictions, or to provide blanket consent to all app downloads and in-app purchases, somehow further the government's legitimate interest in enabling parental control. *Packingham*, 582 U.S. at 106 (content-neutral regulations must not "burden substantially more speech than is necessary to further the government's legitimate interests."). Rather, in addition to imposing burdensome age verification requirements on all Alabamians, the State's approach strips parents of the choice to, for example, trust their 17-year-

old to make his or her own decisions about downloading apps or purchasing books, videos, or music within them.

90. **There Are Less Restrictive Alternatives to the Verification and Consent Requirements.** Insofar as the State's purported interest is in providing parental control, the State entirely disregards the pre-existing and far less restrictive alternatives that already function to achieve the same ends.

91. The CCIA members' major app stores provide more robust (but different) parental control offerings than the Act requires, should parents decide that those offerings should be employed. The Amazon Appstore's Parental Controls feature enables parents to monitor and require parental consent for their children's in-app purchases and to restrict which apps their children have access to.¹⁹ The Google Play Store offers parents the same functionality through its Family Link feature,²⁰ as does the Apple App Store through Screen Time.²¹

92. All of CCIA's member app stores enforce content policy guidelines to ensure that content is age appropriate, and to enable parents to filter their children's exposure to apps and content based on the content rating or tagged content

¹⁹ See *Set Parental Controls for In-App Purchases*, Amazon.com, <https://www.amazon.com/gp/help/customer/display.html?nodeId=GB8P5MQSYFYHPCQ5> (last visited Oct. 15, 2026).

²⁰ *How To Set Up Parental Controls on Google Play*, Google Play Help, <https://support.google.com/googleplay/answer/1075738?hl=en> (last visited Oct. 15, 2026).

²¹ *Use Parental Controls on Your Child's iPhone or iPad*, Apple, <https://support.apple.com/en-us/105121> (last visited Oct. 15, 2026).

categories. Apple, for instance, allows parents to block music, videos, or podcasts that contain explicit content and to prevent access to books, movies, TV shows, and apps with specific content ratings.²² Google Play also allows parents to “choose the highest [content] rating you want to allow for rental, purchase, or playback” of apps, games, movies, and TV shows.²³ The Amazon Appstore will “reject[] or suppress[]” apps that contain content that would not be considered “family-friendly.”²⁴

93. Individual apps on the CCIA members’ app stores also apply and enforce their own content guidelines, as well as provide tools for parents to restrict the content their children may access, and are able to tailor their respective restrictions and other protective tools to the unique content and features available through their services.²⁵

94. Instead of empowering parents to use these tools where they believe them appropriate for their families, the State now subjects *all* users of CCIA’s members’ app stores to an invasive identity verification process and *legally obligates* parents to use the State’s preferred parental tools.

²² *Id.*

²³ *How To Set Up Parental Controls on Google Play*, Google Play Help, <https://support.google.com/googleplay/answer/1075738?hl=en> (last visited Oct. 15, 2026).

²⁴ *Amazon Appstore Content Policy*, Amazon.com, <https://developer.amazon.com/docs/policy-center/understanding-content-policy.html> (last visited Oct. 15, 2026).

²⁵ *See, e.g., Supervised experiences for pre-teens – Understand your choices as a family*, YouTube Help, <https://support.google.com/youtube/answer/10315420> (last visited Oct. 15, 2026); *Parental Controls on Netflix*, Netflix Help Center, <https://help.netflix.com/en/node/264> (last visited Oct. 15, 2026).

95. That app stores are in practice *prohibited* from accepting blanket parental consent further belies the State’s purported goal to return decision-making for children’s online safety back to their parents. Under the Act, the State forces every parent to review and approve every app download and every in-app transaction for every app available.

96. Moreover, Alabama has at least one existing law that is targeted to preventing minors from accessing sexual material harmful to minors online. *See* Ala. Code § 8-19G-3. Alabama law also has longstanding protections for minors who enter into contracts, providing that a minor is not liable on any contract he makes and that he may disaffirm it, subject to limited exceptions not relevant here. *S.B. v. Saint James Sch.*, 959 So. 2d 72, 96 (Ala. 2006). In light of these preexisting regulations and voluntary protective features, the Act goes far beyond any asserted state interest in protecting minors online.

97. **The Act Is Also Underinclusive.** In addition to its overbreadth issues, the Act is wildly underinclusive. The Act targets only apps and app stores on “mobile device[s],” §§ 1(5), (6), (13), and does nothing whatsoever to prevent minors from accessing the same content via a web browser or non-mobile app—or in a brick-and-mortar location. By overregulating mobile apps while ignoring similar or identical content available via web browsers, smart TV apps, and other media, the Act

simultaneously imposes tremendous burdens on speech while failing to serve its own purported state interests.

98. For these reasons, the Act violates the First Amendment rights of CCIA and its app store members. CCIA and its members will also face nonrecoverable compliance costs if the Act is not enjoined. If the Act is not enjoined, CCIA and its members will thus suffer irreparable harm.

COUNT II
42 U.S.C. § 1983; Ex Parte Young
VIOLATION OF THE FIRST AMENDMENT, AS INCORPORATED
AGAINST THE STATES THROUGH THE FOURTEENTH AMENDMENT
(Verification and parental-consent requirements facially to app stores,
Alabama Act No. 2026-59 §§ 1–8)

99. CCIA incorporates all prior paragraphs as if fully set forth herein.

100. **The Act Is Facially Unconstitutional Because a Substantial Number of Its Applications Are Unconstitutional, Judged in Relation to Its Plainly Legitimate Sweep.** A plaintiff bringing a facial First Amendment challenge need not show that a law is invalid in all its applications; rather, the challenger need only establish “that a substantial number of [the law’s] applications are unconstitutional, judged in relation to the statute’s plainly legitimate sweep.” *Moody*, 603 U.S. at 723 (quoting *Americans for Prosperity Found. v. Bonta*, 594 U.S. 595, 615 (2021)). Where, as here, the Act’s “unconstitutional applications substantially outweigh its constitutional ones,” it is facially invalid. *Id.* at 724.

101. The Act Burdens the Dissemination of and Access to Protected Speech at the Threshold for All App Stores. The Act's verification and consent requirements operate as a threshold barrier to constitutionally protected speech for every Alabamian who seeks to access any app store and any app covered by the Act. The burdens imposed by the Act, including the invasive, universal age-verification gate imposed at the threshold of access, before even adults in Alabama can access the myriad protected speech made available on app stores; the parental-tethering and parental-consent regime imposed on minors when they create accounts with app stores; and the repeated notice and consent provisions requiring that app stores renew consent every time a minor seeks to make an in-app purchase or a developer makes a significant change to its app, thus recur in every one of the Act's applications, regardless of which app store is subject to enforcement.

102. The Age-Verification and Parental-Consent Regime Fails Under Any Level of Heightened Scrutiny, Whether Strict or Intermediate. Whether the Act's verification and consent regime is analyzed under strict scrutiny or intermediate scrutiny, it fails either standard (and it fails facially, because the same tailoring defects recur in every application of the Act).

103. The verification and consent provisions similarly would fail because the Act is overbroad in capturing nearly every app within an app store and is underinclusive by failing to impose any gates around web-based or non-mobile

analog. The Act makes no attempt to exempt apps that are irrelevant to the State's cognizable interest, as evidenced by its practical prohibition on parents deciding to provide blanket consent to their children.

104. The Act sweeps in every app made available through any covered store without regard to whether that app implicates the State's asserted interest in protecting minors from harmful content. As a result of this indiscriminate sweep, the State's targeting of protected speech is direct; it would be impossible to interpret in a manner that would narrow the verification and consent provisions' reach to only those applications that further the State's asserted interest in protecting minors. The Act further enlists all app stores to carry out this vast censorship scheme.

105. Accordingly, a substantial number (arguably the entirety, given the CCIA members' app stores' prevalence) of the Act's applications to covered app stores are unconstitutional under the First Amendment, judged in relation to whatever legitimate sweep the Act may have.

106. For these reasons, and for those set forth in Count I, the Act violates the First Amendment rights of CCIA and its members, of their users, and of the app stores the Act purports to regulate generally. Absent injunctive relief, CCIA and its members, along with similarly situated app stores throughout the State, will suffer irreparable harm.

COUNT III
42 U.S.C. § 1983; Ex Parte Young
VIOLATION OF THE FIRST AMENDMENT, AS INCORPORATED
AGAINST THE STATES THROUGH THE FOURTEENTH AMENDMENT
(Verification and parental-consent requirements as-applied to app developers,
Alabama Act No. 2026-59 §§ 1–9)

107. CCIA incorporates all prior paragraphs as if fully set forth herein.

108. **The Verification and Consent Requirements Burden Speech Rights of App Developers.** CCIA members also develop and offer mobile apps that facilitate access to speech, disseminate speech, curate and compile speech, and produce speech themselves, including news, art, photographs, books, music, video, and games. In particular, CCIA’s members develop the following applications: YouTube, Audible, IMDb, Twitch, and Gmail, among others.

109. These apps apply and enforce their own content and policy guidelines and, in some cases, offer curated experiences for younger or more sensitive audiences. For example, Audible offers the ability to create a Kids Profile for parents and guardians concerned about controlling content selections for younger listeners. Parents or guardians can create a Kids Profile in the Audible app and add audiobooks and podcast episodes to their library for their children.

110. Mobile apps facilitate and “engage in a wide array of protected First Amendment activity on topics as diverse as human thought.” *Packingham*, 582 U.S. at 105 (quotation omitted). Those activities involve “publish[ing],” *Reno*, 521 U.S. at 853; “disseminat[ing],” *303 Creative*, 600 U.S. at 594; “creating, distributing,

[and] consuming,” *Brown*, 564 U.S. at 792 n.1; and “compiling and curating” protected speech. *Moody*, 603 U.S. at 731.

111. The Act’s verification and consent regime places a series of interdependent access gates between these apps and their users, creating barriers and in some cases full blocks to users’ ability to access and download apps.

112. Further, the Act creates additional burdens on app developers to independently ensure that the unconstitutional gates are up and functioning. It does so by creating a separate duty on app developers to “verify through the app store’s data sharing methods” both “the age category of users located in [Alabama]” and, “for a minor account, whether verifiable parental consent has been obtained” before the minor can download the app or make an in-app purchase. § 9(a)(1). This creates yet another burden on CCIA member developers because they must verify this information and potentially obtain additional (duplicative) consent from parents before permitting their users to access their apps and content (including every in-app purchase).

113. **The Verification, Consent, and Developer-Verification Requirements Trigger Strict Scrutiny.** As discussed with respect to Count I, the verification and consent regime triggers strict scrutiny because the Act’s purpose is content-based, its all-encompassing sweep restricts an entire medium of expression, and it directly burdens protected speech. Further, the developer-verification

provision (§ 9(a)(1)) conscripts CCIA member developers into policing the app stores' compliance with the law, and presumably cutting off access to their own content if the verification and consent regime is not functioning properly at the app store level.

114. The Verification, Consent, and Developer-Verification Requirements Are Not Substantially Related to the State's Alleged Interest. The Act similarly would fail intermediate scrutiny because it sweeps in huge swaths of protected speech, rather than creating a solution substantially related to the State's asserted interest in protecting children. The Act makes no attempt to exempt apps that are irrelevant to the State's cognizable interest.

115. The Act also disregards clear less restrictive alternatives and existing parental controls at both the app store and individual app level, along with app stores' and developers' existing content policies directed at protecting children, and thus entirely declines to consider capacities that function to achieve the same ends as the Act's purported purpose. There is no reason for the Act to prevent parents from providing blanket consent to certain forms of protected speech such as audiobooks, music, videos, games, or even apps writ large that meet certain age-rating criteria (*e.g.*, age 4+). But because the law in practice prevents that functionality, *see* §§ 1(17), 3(2), parental approval will be required for a minor—even a 17-year-old—to

download Libby and listen to *The Cat in the Hat* or *Where the Wild Things Are*. Its requirements are both burdensome and unnecessary.

116. The verification and consent provisions are also wildly underinclusive. For example, they heavily burden a person's ability to browse audiobooks on a mobile app (such as Audible) but do nothing to restrict their access to the same content on a website (like Audible.com). In ignoring content available via web browsers, smart TV apps, and other media, while heavily burdening app developers, the Act simultaneously imposes tremendous burdens on speech while failing to serve its own purported state interests.

117. For these reasons, the Act violates the First Amendment rights of CCIA and its developer members. CCIA and its members will also face nonrecoverable compliance costs if the Act is not enjoined. If the Act is not enjoined, CCIA and its members will thus suffer irreparable harm.

COUNT IV

42 U.S.C. § 1983; Ex Parte Young

VIOLATION OF THE FIRST AMENDMENT, AS INCORPORATED AGAINST THE STATES THROUGH THE FOURTEENTH AMENDMENT (Age rating requirements as-applied to developers, Alabama Act No. 2026-59, §§ 1; 9(a)(2)–(5), (c)(2); 12(b))

118. CCIA incorporates all prior paragraphs as if fully set forth herein.

119. The Act could, but should not, be read to require app developers, including CCIA members, to assign each app and each in-app purchase (e.g., every

movie available for rent on Prime Video) an age rating based on the Act's four predetermined age categories and to provide a content description justifying those ratings. The Act does not provide any objective criteria for determining whether an app or in-app purchase falls into a given age category—nor could it. The Act also requires app developers to notify app stores any time they make a “significant change” to the app, including when they change the age category of an app or the “content elements or functions” that led to that rating. §§ 1(19), 9(a)(2). Developers may be held liable for knowingly misrepresenting the age ratings contained in the parental consent disclosure. § 9(c)(2).

120. To the extent the Act is read to require app developers to age-rate their apps and in-app purchases and disclose the basis for those decisions, it violates the First Amendment. This requirement would compel CCIA members as app developers to engage in speech that they do not and would not otherwise make on two levels: ratings of apps and ratings of in-app purchases.

121. At the app store level, while CCIA's app store members currently implement their own content-ratings at the app level, the Act could be read to, in practice, require developers to rate their apps in line with the Act's age categories and provide those ratings (and justifications for those ratings) to app stores for purposes of parental consent disclosures. Specifically, the Act holds developers liable for knowing misrepresentations in the parental consent disclosure, including

any age rating in that disclosure. § 9(c)(2). But a developer is not liable for a violation of that section if the developer uses widely adopted industry standards to determine the app’s *age category* and the *content description* disclosures, § 12(b) (emphases added). This could be interpreted to mean that app developers are only entitled to this safe harbor if they use the State’s prescribed four-tiered age rating scheme. *See* § 1(2). Under this reading, in order to ensure they are not held liable for any age rating disclosed in the parental disclosure, developers would effectively be compelled to re-rate their own apps and any in-app content according to the Act’s prescribed age categories and to provide justifications for their rating decisions to the app stores for purposes of parental consent disclosures.

122. At the level of apps themselves, the Act also requires that developers limit their use of the age verification data received from app stores to “enforce developer-created age-related restrictions, protections, or defaults” and “implement safety-related features or defaults.” § 9(a)(3). This could, but should not, be read to require developers to rely on the Act’s arbitrary age buckets if they choose to set age ratings for any of the in-app content they offer.

123. This age-rating and content description requirement would burden app developers’ protected speech thrice over. *First*, it would impose a content-based burden on speech by “[m]andating speech that a speaker would not otherwise make[.]” *Riley v. Nat’l Fed’n of Blind of N. Carolina, Inc.*, 487 U.S. 781, 795 (1988).

Second, the requirement would “deputize[] covered businesses into serving as censors for the State.” *NetChoice, LLC v. Bonta*, 113 F.4th 1101, 1118 (9th Cir. 2024) (citing *Interstate Cir., Inc. v. City of Dallas*, 390 U.S. 676, 678, 684 (1968)). *Finally*, the age-rating requirement would force app developers to forgo their existing rating regimes in favor of the Act’s, thereby infringing upon their editorial and curatorial rights. To the extent Alabama intends to adopt this interpretation of Act 2026-59, Alabama seeks to overwrite the existing content rating systems used by apps that disseminate third-party speech (e.g., YouTube,²⁶ Prime Video) with its own state-mandated rating system.

124. **The Age-Rating and Content Description Requirement Would Be Subject to Strict Scrutiny.** Content-based regulations of non-commercial speech must satisfy strict scrutiny. *First*, the speech at issue (age ratings) is not commercial speech because it is not “related solely to the economic interests of the speaker and its audience,” *Book People*, 91 F.4th at 339 (citation omitted), and it “does [] more than propose a commercial transaction,” *United States v. United Foods, Inc.*, 533 U.S. 405, 409 (2001).

125. *Second*, even a regulation compelling commercial speech receives “at minimum, intermediate scrutiny,” and only where it “compels commercial

²⁶ YouTube applies content rating labels to paid content. Those ratings are Strong Language (L), Nudity (N), Sexual Situations (S), Violence/Disturbing (V), Drug use (D), Flashing Lights (F). *YouTube content rating*, YouTube Help, <https://support.google.com/youtube/answer/146399?hl=en> (last visited Oct. 15, 2026).

enterprises to disclose purely factual and uncontroversial information about their services” can it receive anything less. *Free Speech Coal., Inc. v. Paxton*, 95 F.4th 263, 283 (5th Cir.), *cert. granted*, 144 S. Ct. 2714, *and aff’d*, 606 U.S. 461 (2025). To the extent the Act compels age rating and disclosure of content descriptions, that requirement far exceeds the “purely factual” disclosures required by *Zauderer*. *Zauderer v. Off. of Disciplinary Couns. of Supreme Ct. of Ohio*, 471 U.S. 626, 651 (1985). That is because the Act would require CCIA developer members to undergo a subjective analysis and determine—based on an app’s expressive content—which age category their app, and any in-app purchase, falls within, then disclose the basis of the developer’s conclusion. That task is highly subjective, and arguably impossible, for mobile apps that host a wide array of third-party content for all age groups and that allow in-app downloads of speech such as books, music, television shows, and games. *See, e.g., Book People*, 91 F.4th at 340 (holding that state-mandated content ratings for books are “neither factual nor uncontroversial”); *Schwarzenegger*, 556 F.3d at 953 (age-labeling scheme for video games); *Blagojevich*, 469 F.3d at 652 (same).

126. *Third*, if the Act is read to require age rating and disclosure of those ratings and their justifications, that requirement is unduly burdensome, *Nat’l Inst. of Fam. & Life Advoc. v. Becerra*, 585 U.S. 755, 776 (2018), because developers must categorize each age-rated app and in-app purchase into one of four arbitrary age

categories, or else risk being held liable for their knowing misrepresentation. Not only will this take considerable time and resources to accomplish, but the Act fails to provide any criteria for making the rating determination (despite requiring that the developers then publicly disclose their criteria). Moreover, existing industry standards, such as the ESRB guidelines, are at odds with the Act's age categories.

127. The Age-Rating and Content Description Provisions Would Fail Under Any Level of Scrutiny. Such an age-rating and content description requirement is overbroad and not narrowly tailored. It encompasses nearly every app and in-app purchase, regardless of whether the app engages in pure speech (such as numerous CCIA members' apps) or unprotected speech; regardless of whether the app hosts a wealth of third-party speech that would render the age rating meaningless or impossibly burdensome; and regardless of whether the app pertains to activities far afield from the State's purported interests.

128. The Act also fails to recognize—and directly conflicts with—existing age-rating standards. As discussed, all app stores have elaborate content rating systems, and the vast majority of their preexisting age categories do not line up with the Act's. Similarly, in addition to app-level content ratings, some apps—including CCIA member apps—use their own content rating systems for content published within their apps. The State has no place, and no interest, in overwriting a long-

standing system of content ratings with its impermissibly vague and wholly untested age categories.

129. Such an age-rating requirement also fosters self-censorship by app developers who will want to (1) achieve the lowest possible age rating to avoid discouraging users from downloading their apps and appeal to the largest possible audience; (2) refrain from making certain changes to their apps that would trigger a change in its age rating and thus the need to notify app stores; and (3) engage in content-moderation practices designed to achieve the pre-determined age rating, for apps that host third-party content.

130. Accordingly, to the extent the Act is properly interpreted to require developers to rate their apps and in-app purchases in compliance with the Act's age categories and disclose those ratings and their justifications, that requirement impermissibly and unnecessarily compels speech. Both alone and in tandem with the verification and consent regime, this requirement would violate the First Amendment and CCIA members' First Amendment rights.

131. For these reasons, the Act violates the First Amendment rights of CCIA and its members. CCIA and its members will also face nonrecoverable compliance costs if the Act is not enjoined. If the Act is not enjoined, CCIA and its members will thus suffer irreparable harm.

COUNT V
42 U.S.C. § 1983; Ex Parte Young
VOID FOR VAGUENESS UNDER THE FIRST AND FOURTEENTH
AMENDMENTS
(App Developers: Age-rating and disclosure requirements, Alabama Act No.
2026-59 §§ 1; 9(a)(2)–(5), (c)(2); 12(b))

132. CCIA incorporates all prior paragraphs as if fully set forth herein.

133. To the extent the Act imposes age-rating and disclosure requirements on app developers, those requirements are unconstitutionally vague, as evidenced by the fact that they are, in significant part, implied. That vagueness will chill the publication and dissemination of protected speech.

134. “A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required.” *F.C.C. v. Fox Television Stations, Inc.*, 567 U.S. 239, 253 (2012). Despite this, the Act makes it impossible for app developers to ascertain their obligations under the law.

135. The Act has a glaring omission that mars the State’s effort entirely: it does not clearly create any obligation for any entity to adopt the age ratings set forth in § 1(2), but it simultaneously could be read to impose liability for failure to do so. On the one hand, the Act holds *developers* liable for “knowingly misrepresent[ing] [the] information in the parental consent disclosure,” § 9(c)(2), including age ratings. On the other hand, the Act requires that *app stores*, not developers, provide the

parental consent disclosure. §§ 1(17), 3(2). The Act’s other provisions only exacerbate the unclear compliance obligations imposed on developers by these provisions. While the Act requires app stores to include age ratings and content descriptions in the parental consent disclosure only “if available,” § 1(17)(d)–(e), it simultaneously provides that developers are entitled to a safe harbor from liability for that provision if they use “widely adopted industry standards to determine the app’s age category and content description,” and “appl[y] those standards consistently and in good faith,” § 12(b). The Act provides no guidance to developers regarding what information developers must provide to app stores for purposes of the parental consent disclosure, or what constitutes a developer’s knowing misrepresentation in a disclosure that developers are not responsible for giving.

136. Further, as discussed *supra* ¶ 36, app stores have existing, voluntary age-rating standards for apps that directly conflict with the Act’s age categories. The Act, which requires app stores to disclose age ratings, if available, as a precondition to procuring parental consent, § 1(17)(d), thus could be read to require app stores to disclose multiple conflicting age ratings. First, the app store might be required to disclose *the app store’s* preexisting age ratings in the parental consent disclosure, given that those ratings are available to app stores. But the Act also in practice provides that *developers* should set specific “age categories,” meaning the Act’s age ratings, for their own apps and provide that information to the app stores in order to

benefit from the Act’s safe harbor. Two conflicting age ratings for a particular app will thus sometimes be “available” to app stores, but the Act provides absolutely no guidance regarding how those ratings must be disclosed and what constitutes a “knowing[] misrepresent[ation]” by an app store or developer in those circumstances. These provisions are so vague that they do not “give the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly,” a particular concern in the First Amendment context. *Pine v. City of W. Palm Beach*, 762 F.3d 1262, 1275 (11th Cir. 2014).

137. In addition to the incomprehensible obligations imposed on developers in the context of the parental consent disclosure, the Act also requires that developers, to “comply with applicable law,” “[r]equest age category data or verifiable parental consent” from app stores, which have collected that data in line with the Act’s age categories. § 9(a)(4). The Act simultaneously provides that developers must limit their use of that data to certain specified purposes, i.e., “ensur[ing] compliance with applicable laws or regulations,” along with “enforc[ing] developer-created age-related restrictions, protections, or defaults,” and “implement[ing] safety-related features or defaults,” § 9(a)(3), such as app and in-app content age ratings. However, the Act *also* requires that developers “use the lowest age category indicated by” either the age verification data provided by the app store *or the age data independently collected by the developer* when

implementing any developer-created safety-related features or defaults. § 9(a)(5). This will necessarily impose conflicting obligations on developers in some cases. For example, if an app developer has collected age data for a user indicating that user is 55 years old, but the age verification data provided by the app store indicates the user is 15 years old, the requirement that developers rely on the *lower* of those two ages would make it impossible for a developer to treat that 55-year-old user as an adult. The developer would be unable to enforce a safety-related feature or age rating intended to limit that adult user's ability to send unsolicited messages to minors.

138. Finally, the Act provides *no guidance* for developers on how to set age ratings in compliance with the law beyond creating age categories that clash with other standards. § 1(2). And while the Act provides a safe harbor for developers who “use[] widely adopted industry standards” to set their apps’ age categories, again, those age categories conflict with other standards, making compliance with this provision hopelessly opaque if not impossible. *See* §§ 1(2), 12(b).

139. These amorphous standards also raise concerns about disparate enforcement.

140. This lack of guidance, combined with the imposition of liability, threatens to undermine the age rating and disclosure system imposed by the Act. To the extent the rating system forces each app developer to determine its app’s age

rating on an app-wide basis with the exception of in-app purchases, §§ 1(8), 1(17), 3(2), developers of apps like Prime Video will be strongly incentivized to rate their apps in compliance with the Act's age categories according to the most mature accessible content available for purchase, to mitigate risk of being accused of "knowingly misrepresenting" the app's age rating or facilitating a minor's access to inappropriate content. The perverse result is that an app with ample content created specifically for children²⁷ may be rated for adults aged 18 and older. And this principle applies equally to any app that distributes content without in-app purchases, such as Netflix, Hulu, and the like. (Query how a news app, which often discusses or portrays violent or gruesome content, fits in.)

141. Thus, without clear guidance, apps will not know what content they should censor, and they will likely err on the side of over-censoring, thus chilling protected speech. The incentives in favor of over-censorship will also affect the accuracy of information disclosed for parental consent and may lead parents to deny access to apps that would otherwise be appropriate for children due to an over-inflated age rating.

142. For these reasons, the Act violates the constitutional rights of CCIA and its members. CCIA and its members will also face nonrecoverable compliance costs

²⁷ *Kids*, Prime Video, <https://www.amazon.com/gp/video/kids> (last visited Oct. 15, 2026).

if the Act is not enjoined. If the Act is not enjoined, CCIA and its members will thus suffer irreparable harm.

COUNT VI

42 U.S.C. § 1983; Ex Parte Young

**VOID FOR VAGUENESS UNDER THE FIRST AND FOURTEENTH
AMENDMENTS**

**(App Developers: Notice of significant changes requirement, Alabama Act No.
2026-59 §§ 1, 3(1)–(2), 4, 8(2), 9(a)(2))**

143. CCIA incorporates all prior paragraphs as if fully set forth herein.

144. The Act further requires developers to “notify app store providers of any significant change to an app.” § 9(a)(2). A change is significant if it is “[a] material modification to [the] app’s terms of service or privacy policy” that “[c]hanges the categories of data collected, stored, or shared,” “[a]lters the app’s age rating or content descriptions,” or adds “new monetization features” including “in-app purchases” or “advertisements,” where no such features were previously present. § 1(19).

145. These triggers are wide-ranging and unclear. The Act does not define what a “material modification” might include. Nor does it explain whether a “new monetization feature” covers a category of goods or requires notice for each new genre of song, book, movie, or item added to a repository like Apple Music, Audible, or Prime Video, or new types of content monetized on YouTube using ContentID. Similarly, the “advertisements” presented in apps constantly change—so does each

new category of ad trigger a new notice requirement? The Act’s lack of guidance on these points and others means that developers will not have “a reasonable opportunity to know what is prohibited, so that [they] may act accordingly.” *Book People, Inc. v. Wong*, 692 F. Supp. 3d 660, 695 (W.D. Tex. 2023) (quoting *Roark & Hardee LP v. City of Austin*, 522 F.3d 533, 548, 551 (5th Cir. 2008)), *vacated and aff’d in part on other grounds*, 91 F.4th 318, *reh’g denied*, 98 F.4th 657 (5th Cir. 2024).

146. The law can thus be construed to require near-constant notifications from developers to app stores. And because each notification requires app stores to notify users of the significant change and revoke a minor’s access to the app while the app store refreshes parental consent, *see* §§ 4, 8(2), this provision threatens to impose severe restraints on developers’ and users’ speech.

147. This lack of guidance presents opportunities for arbitrary or selective enforcement, incentivizes over-censorship, and utterly fails to satisfy the heightened notice standards required of laws that “interfere[] with the right of free speech.” *Vill. of Hoffman Ests. v. Flipside, Hoffman Ests., Inc.*, 455 U.S. 489, 499 (1982).

148. Unless declared invalid and enjoined, the notice of significant changes requirement will for this additional reason unlawfully deprive app developers of their First Amendment and Due Process rights, causing them to suffer irreparable injuries.

149. For these reasons, the Act violates the constitutional rights of CCIA and its members. CCIA and its members will also face nonrecoverable compliance costs if the Act is not enjoined. If the Act is not enjoined, CCIA and its members will thus suffer irreparable harm.

COUNT VII
42 U.S.C. § 1983; Ex Parte Young
VIOLATION OF THE COMMERCE CLAUSE OF THE UNITED STATES
CONSTITUTION

150. CCIA incorporates all prior paragraphs as if fully set forth herein.

151. The Act violates the Commerce Clause under *Pike v. Bruce Church, Inc.*, 397 U.S. 137 (1970), and its progeny because it imposes an unreasonable and undue burden on interstate commerce that is clearly excessive in relation to any local benefit conferred on the State of Alabama. It is also likely to subject businesses to inconsistent state regulations.

152. The Act burdens interstate commerce by deterring online service providers from offering services available across state lines, or else limiting the types of services available within and across the United States. This is because app stores and the apps they publish are accessible globally, and whether a covered business wishes to avoid Alabama's regulations or comply with them, doing so inherently requires both app stores and developers to degrade or withdraw their services for all users in all states.

153. The Act also burdens interstate commerce by forcing app stores to comply with an inconsistent patchwork of state rules. For example, the Act will in practice require covered businesses to adopt verification tools that might violate other states' conflicting privacy laws (such as biometric privacy laws). Similarly, the Act could be read to effectively require app developers to rate their apps, and all content available for purchase through those apps, in line with the age categories provided by the Act, without regard to any different or conflicting age ratings app developers have adopted or might be required to adopt in other states.

154. The Alabama Legislature has not identified any local interest sufficient to justify these onerous impositions on interstate commerce. And to the extent that the Act purports to protect minors, its protections are wholly ineffective because minors can access much of the same content that exists on apps from their website counterparts. Therefore, even if Alabama's interest were deemed sufficiently local, the Act's drastic impositions on interstate and online commerce far outweigh what little the Act does to further that purpose.

155. The Act also violates the Commerce Clause because it regulates extraterritorially in violation of *Healy v. Beer Institute, Inc.*, 491 U.S. 324, 336 (1989). For the same reasons that the Act burdens interstate commerce by depressing or degrading the output and quality of apps available nationwide, it necessarily has the practical and per se unconstitutional effect of regulating commercial and speech-

related activities that occur wholly outside Alabama, such as by causing an app developer based in California to withhold a product or service to users in Florida due to the costs imposed by the Alabama statute.

156. Unless declared invalid and enjoined, the Act will operate to unconstitutionally burden interstate commerce in violation of the Commerce Clause.

COUNT VIII
Ex Parte Young
EQUITABLE RELIEF

157. CCIA incorporates all prior paragraphs as if fully set forth herein.

158. The Act, including the challenged provisions, violates federal law both facially and as-applied, and deprives Plaintiff, its members, and its members' users of enforceable rights guaranteed by federal law. Federal courts have the power to enjoin unlawful actions by state officials. *Armstrong v. Exceptional Child Ctr.*, 575 U.S. 320, 326–27 (2015).

159. This Court can and should exercise its equitable power to enter an injunction precluding Defendant from enforcing the Act against Plaintiff's members.

COUNT IX
DECLARATORY RELIEF

160. CCIA incorporates all prior paragraphs as if fully set forth herein.

161. Sections 1–9, 11, and 12 of the Act violate the First and Fourteenth Amendments of the Constitution and thereby deprive Plaintiff, its members, and its members' users of enforceable rights.

162. With exceptions not relevant here, in any “case of actual controversy within [their] jurisdiction,” federal courts have the power to “declare the rights and other legal relations of any interested party seeking such declaration.” 28 U.S.C. § 2201(a).

163. This Court can and should exercise its equitable power to enter a declaration that the challenged provisions of the Act are unconstitutional and otherwise unlawful, both facially and as-applied.

PRAYER FOR RELIEF

Plaintiff respectfully requests an order and judgment:

- A. Declaring that Alabama Act No. 2026-59 §§ 1–9 are unlawful;
- B. Declaring that Alabama Act No. 2026-59 §§ 1–9 violate the First Amendment to the Constitution as applied to CCIA’s members;
- C. Declaring that Alabama Act No. 2026-59 §§ 1–8 facially violate the First Amendment to the Constitution;
- D. Declaring that Alabama Act No. 2026-59 §§ 1, 8(2), 9(a)(2)–(5), 9(c)(2), 12(b) do not require developers to age-rate apps and in-app purchases or to use the Act’s age categories to do so;
- E. Declaring that Alabama Act No. 2026-59 §§ 3(1)–(2), 4, 8(2), 9(a)(2)–(5), (c)(2), 12(b) are void for vagueness;
- F. Declaring that the entire Act is preempted by the Commerce Clause;

- G. Enjoining Defendant and his agents, employees, and all persons acting under their direction or control from taking any action to enforce the challenged portions of the Act against Plaintiff's members;
- H. Entering judgment in favor of Plaintiff;
- I. Awarding CCIA its attorneys' fees and costs incurred in bringing this action, including attorneys' fees and costs under 42 U.S.C. § 1988(b) for successful 42 U.S.C. § 1983 claims against state officials; and
- J. Awarding Plaintiff all other such relief as the Court deems just and proper.

Dated: October 28, 2026

Respectfully submitted,

/s/ J. Evans Bailey

Brian Willen*
Edward Percarpio*
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
31 West 52nd Street, Fifth Floor
New York, NY 10019
Tel: 212-999-5800
bwillen@wsgr.com
epercarpio@wsgr.com

J. Evans Bailey
RUSHTON, STAKELY, JOHNSTON &
GARRETT, P.A.
P.O. Box 270
Montgomery, AL 36101-0270
Tel: 334-206-3100
ebailey@rushtonstakely.com

Elizabeth Sharkey*
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
1700 K Street NW, Fifth Floor
Washington, DC 20006
Tel: 202-973-8800
esharkey@wsgr.com

Lauren Gallo White*
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
One Market Plaza
Spear Tower, Suite 3300
San Francisco, CA 94105
Tel: 415-947-2000
lwhite@wsgr.com

*Attorneys for Plaintiff Computer &
Communications Industry Association*

**pro hac vice application forthcoming*

EXHIBIT A



ACT #2026- 59

1 HB161
2 V7D54VP-3
3 By Representatives Sells, Mooney
4 RFD: State Government
5 First Read: 13-Jan-26





HB161 Enrolled

1 Enrolled, An Act,

2 Relating to consumer protection; to require an app
3 store provider to take certain actions regarding age
4 verification, parental notification, and data protection; to
5 prohibit an app store provider or developer from taking
6 certain actions that allow minors to access apps without
7 parental consent; to require the Attorney General to adopt
8 rules; and to authorize the Attorney General to bring an
9 action for a violation as a deceptive trade practice.

10 BE IT ENACTED BY THE LEGISLATURE OF ALABAMA:

11 Section 1. For the purposes of this act, the following
12 terms have the following meanings:

13 (1) ACCOUNT HOLDER. The individual associated with a
14 mobile device.

15 (2) AGE CATEGORY. Whether an individual is: (i) under
16 13 years of age; (ii) at least 13 years of age but less than
17 16 years of age; (iii) at least 16 years of age but less than
18 18 years of age; or (iv) at least 18 years of age.

19 (3) AGE CATEGORY DATA. Information about a user's age
20 category which is collected by an app store developer and
21 shared with a developer.

22 (4) AGE RATING. A classification that assesses the
23 suitability of an app's content and functions for different
24 age groups.

25 (5) APP. A software application or electronic service
26 that a user may run or direct on a mobile device. The term
27 includes pre-installed apps.

28 (6) APP STORE. A publicly available website, software

**HB161 Enrolled**

29 application, or electronic service that allows account holders
30 to download apps from third-party developers onto a mobile
31 device.

32 (7) APP STORE PROVIDER. An entity that owns, operates,
33 or controls an app store that allows account holders in the
34 state to download apps onto a mobile device.

35 (8) CONTENT DESCRIPTION. A description of the specific
36 content elements or functions that inform an app's age rating.

37 (9) DEVELOPER. An entity that owns or controls an app
38 made available through an app store or a pre-installed app.

39 (10) IN-APP PURCHASE. A charge associated with any user
40 conduct within an app and billed by an app store, including,
41 but not limited to, the acquisition of virtual currency,
42 digital goods, digital services, or other apps.

43 (11) MINOR. An individual under 18 years of age, unless
44 the individual is married or legally emancipated.

45 (12) MINOR ACCOUNT. An account with an app store
46 provider that is established by an individual who the app
47 store provider has determined is a minor.

48 (13) MOBILE DEVICE. A phone or general-purpose tablet
49 that: (i) provides cellular or wireless connectivity; (ii) is
50 capable of connecting to the Internet; (iii) runs a mobile
51 operating system; and (iv) is capable of running apps through
52 the mobile operating system.

53 (14) MOBILE OPERATING SYSTEM. Software that: (i)
54 manages mobile device hardware resources; (ii) provides common
55 services for mobile device programs; (iii) controls memory
56 allocation; and (iv) provides interfaces for apps to access



HB161 Enrolled

device functionality.

(15) PARENT. With respect to a minor, any of the following individuals:

a. A biological parent.

b. A legal guardian.

c. An individual with legal custody.

(16) PARENT ACCOUNT. An account with an app store provider which is affiliated with one or more minor accounts and which is verified to have been established by an individual who the app store provider has determined is not a minor.

(17) PARENTAL CONSENT DISCLOSURE. The following information that an app store provider is required to provide to a parent before obtaining parental disclosure:

a. A description of the personal data collected by the app from a user.

b. A description of the personal data shared by the app with any third party.

c. Any methods implemented by the developer to protect personal data.

d. The age rating of the app or in-app purchase, if available.

e. The content description of the app or in-app purchase, if available.

(18) PRE-INSTALLED APP. Any app, or portion of an app, that is present on a mobile device at the time of purchase, initial activation, or first use by the consumer. The term includes, but is not limited to: (i) browsers; (ii) search



HB161 Enrolled

85 engines; (iii) messaging apps; and (iv) other apps, or
86 portions of apps, that are installed or partially installed by
87 the device manufacturer, wireless services provider, retailer,
88 or any other party prior to the purchase, initial activation,
89 or first use of the device by the customer and that may be
90 updated thereafter. The term does not include: (i) core
91 operating system functions; (ii) essential device drivers; and
92 (iii) applications necessary for basic device operation such
93 as phone and settings applications.

94 (19) SIGNIFICANT CHANGE. A material modification to an
95 app's terms of service or privacy policy which does any of the
96 following:

97 a. Changes the categories of data collected, stored, or
98 shared.

99 b. Adds new monetization features, including, but not
100 limited to, in-app purchases or advertisements, where no such
101 features were previously present.

102 c. Alters the app's age rating or content descriptions.

103 (20) VERIFIABLE PARENTAL CONSENT. Authorization that
104 meets all of the following criteria:

105 a. Is provided by an individual who the app store
106 provider has verified is at least 18 years of age.

107 b. Is given after the app store provider has clearly
108 and conspicuously provided the parental consent disclosure to
109 the individual.

110 c. Requires the parent to make an affirmative choice to
111 either grant consent or decline consent.

112 Section 2. (a) An app store provider shall do both of



HB161 Enrolled

the following when an individual located in this state creates an account with the app store provider, or before October 1, 2027, for all accounts in existence on October 2, 2026:

(1) Request age category information from the individual.

(2) Verify the individual's age category using one of the following:

a. Commercially available methods that are reasonably designed to ensure accuracy.

b. An age verification system that complies with rules adopted pursuant to this act.

(b) For the purposes of this section, a method is commercially available if the method includes both: (i) affirmative age attestation by an individual who is reasonably believed to be the parent or legal guardian of the minor; and (ii) other information collected in the ordinary course of account creation or use.

Section 3. An app store provider shall do all of the following when an individual is determined to be a minor pursuant to Section 1:

(1) Require the account to be affiliated with a parent account.

(2) Obtain verifiable parental consent from the holder of the affiliated parent account before allowing the minor to: (i) download an app; (ii) purchase an app; or (iii) make an in-app purchase.

(3) Provide a mechanism for the holder of the affiliated parent account to withdraw consent and notify



HB161 Enrolled

141 developers when the holder of a parent account withdraws
142 consent.

143 Section 4. An app store provider shall do both of the
144 following after receiving notice of a significant change from
145 a developer:

- 146 (1) Notify the user of the significant change.
- 147 (2) For a minor account, do both of the following:
- 148 a. Notify the holder of the affiliated parent account.
- 149 b. Obtain renewed verifiable parental consent before
150 providing access to the significantly changed version of the
151 app.

152 Section 5. An app store provider shall provide
153 developers with real-time access to both of the following:

- 154 (1) Age category data for each user located in this
155 state.
- 156 (2) The status of verifiable parental consent for each
157 minor located in this state.

158 Section 6. An app store provider shall protect personal
159 age verification data by doing both of the following: .

- 160 (1) Limiting the collection and processing to data
161 necessary to: (i) verify a user's age; (ii) obtain parental
162 consent; or (iii) maintain compliance records.
- 163 (2) Transmitting personal age verification data using
164 industry-standard encryption protocols that ensure data
165 integrity and data confidentiality.

166 Section 7. An app store provider shall do both of the
167 following with respect to pre-installed apps:

- 168 (1) Provide available age category information in



HB161 Enrolled

169 response to a request from a developer.

170 (2) Take reasonable measures to facilitate verifiable
171 parental consent for use of a pre-installed app in response to
172 a request from a developer.

173 Section 8. An app store provider may not do any of the
174 following:

175 (1) Enforce a contract or terms of service against a
176 minor unless the app store provider has obtained verifiable
177 parental consent.

178 (2) Knowingly misrepresent the information in the
179 parental consent disclosure.

180 (3) Share age category data or any other associated
181 data except as required by law or as required by this act
182 between an app store provider and a developer.

183 Section 9. (a) A developer shall do all of the
184 following:

185 (1) Verify through the app store's data sharing
186 methods: (i) the age category of users located in this state;
187 and (ii) for a minor account, whether verifiable parental
188 consent has been obtained.

189 (2) Notify app store providers of any significant
190 change to an app.

191 (3) Limit use of age category data received from an app
192 store provider to: (i) enforce developer-created age-related
193 restrictions, protections, or defaults; (ii) ensure compliance
194 with applicable laws or regulations; or (iii) implement
195 safety-related features or defaults.

196 (4) Request age category data or verifiable parental



HB161 Enrolled

consent in all of the following scenarios:

a. Whenever an account holder does any of the following:

1. Downloads an app.
2. Purchases an app.
3. Launches a pre-installed app for the first time.
- b. When implementing a significant change to an app.
- c. To comply with applicable law.

(5) When implementing any developer-created age-related restrictions, safety-related features, or defaults, use the lowest age category indicated by either: (i) age category data received through the app store's data sharing methods; or (ii) age data independently collected by the developer.

(b) A developer may request age category data in any of the following scenarios:

(1) No more than once during each 12-month period to verify either of the following:

a. The accuracy of age category data associated with an account holder.

b. Continued account use within the age category.

(2) When there is reasonable suspicion of either of the following:

a. Account transfer.

b. Misuse outside of the age category.

(3) At the time an account holder creates a new account with the developer.

(c) A developer may not do any of the following:

(1) Enforce a contract or terms of service against a



HB161 Enrolled

225 minor unless the developer has verified through the app store
226 provider that verifiable parental consent has been obtained.

227 (2) Knowingly misrepresent any information in the
228 parental consent disclosure.

229 (3) Share age category data with any person.

230 Section 10. The Attorney General shall adopt rules
231 establishing processes and means by which an app store
232 provider may verify whether an account holder is a minor in
233 accordance with this act.

234 Section 11. (a) Any knowing or reckless violation of
235 this act is deemed a deceptive trade practice actionable under
236 Chapter 19 of Title 8 of the Code of Alabama 1975. Provided,
237 however, the Attorney General shall have the exclusive
238 jurisdiction to bring an action pursuant to Chapter 19 of
239 Title 8, Code of Alabama 1975. If the Attorney General has
240 reason to believe that an entity is in violation of this act,
241 the Attorney General may bring an action against the entity
242 for an unfair or deceptive trade practice. In addition to
243 other remedies available under Chapter 19 of Title 8 of the
244 Code of Alabama 1975, the Attorney General may collect a civil
245 penalty of up to seven thousand five hundred dollars (\$7,500)
246 per violation, reasonable attorney fees, and court costs.

247 (b) If a violation described in subsection (a) is part
248 of a consistent pattern of knowing or reckless conduct, the
249 Attorney General may seek punitive damages against the entity.

250 (c) An action for a claim under this section must be
251 brought within one year from the date the Attorney General
252 knew or reasonably should have known of the alleged violation.



HB161 Enrolled

(d) This section does not preclude any other available remedy at law or equity.

Section 12. (a) A developer is not liable for a violation of this act if the developer demonstrates all of the following:

(1) The developer relied in good faith on applicable age category data received through an app store's data sharing methods.

(2) The developer relied in good faith on notification from an app store provider that verifiable parental consent was obtained.

(3) The developer complied with the requirements of this act.

(b) A developer is not liable for a violation of Section 9(c)(2) if the developer: (i) uses widely adopted industry standards to determine the app's age category and content description; and (ii) applies those standards consistently and in good faith.

(c) Notwithstanding subsection (a), the safe harbor provision applies only to actions brought under this act and does not limit a developer or app store provider's liability under any other applicable law.

(d) An app store provider shall not be liable for a violation of this act if the app store provider generates an erroneous age category signal for a user as long as the app store provider demonstrates that the app store provider did all of the following:

(1) Used a commercially reasonable age verification



HB161 Enrolled

281 process.

282 (2) Exercised due care in conducting the age
283 verification process.

284 (3) Made reasonable efforts to reconcile any
285 discrepancies between a parent's attestation of the minor's
286 age and other age data collected in the ordinary course of
287 account creation or use.

288 Section 13. Nothing in this act shall be construed to
289 do any of the following:

290 (1) Prevent an app store provider or developer from
291 taking reasonable measures to do any of the following:

292 a. Block, detect, or prevent distribution to minors of:
293 (i) unlawful material; (ii) obscene material; or (iii) other
294 harmful material.

295 b. Block or filter spam.

296 c. Prevent criminal activity.

297 d. Protect app store or app security.

298 (2) Require an app store provider or developer to
299 disclose user information to a developer beyond age category
300 or verification of parental consent status.

301 (3) Allow an app store provider or developer to
302 implement measures required by this act in a manner that is:
303 (i) arbitrary; (ii) capricious; (iii) anticompetitive; or (iv)
304 unlawful.

305 (4) Require a developer to collect, retain, reidentify,
306 or link any information beyond what is both:

307 a. Necessary to verify age category data as required by
308 this act; and



HB161 Enrolled

309 b. Collected, retained, reidentified, or linked in the
310 developer's ordinary course of business.

311 (5) Require an app store provider or developer to block
312 access to an application that an account holder has downloaded
313 or installed onto a mobile device prior to October 1, 2026,
314 except to the extent that either:

315 a. A parent account revokes verifiable consent for an
316 affiliated minor account; or

317 b. There has been a significant change to the
318 application.

319 Section 14. Nothing in this act shall be construed to
320 relieve any person from compliance with any other law of this
321 state that requires age verification.

322 Section 15. This act shall become effective on January
323 1, 2027.

HB161 Enrolled



Speaker of the House of Representatives

President and Presiding Officer of the Senate

House of Representatives

I hereby certify that the within Act originated in and
was passed by the House 22-Jan-26, as amended.

John Treadwell
Clerk

Senate	<u>05-Feb-26</u>	Amended and Passed
House	<u>10-Feb-26</u>	Concurred in Senate Amendment

APPROVED

2-17-2026

TIME

10:30 am

Kay Ivey
GOVERNOR

Alabama Secretary Of State

Act Num.....: 2026-59
Bill Num....: H-161

Recv'd 02/17/26 01:00pmMQC

ENGROSSED

SPONSOR

Sells

CO-SPONSORS

Mooney

HOUSE ACTION

I HEREBY CERTIFY THAT THE
RESOLUTION AS REQUIRED IN
SECTION C OF ACT NO. 81-889
WAS ADOPTED AND IS ATTACHED
TO THE BILL, H.B. 1601

YEAS 94 NAYS 0

JOHN TREADWELL, Clerk

I HEREBY CERTIFY THAT THE
NOTICE & PROOF IS ATTACHED
TO THE BILL, H.B. 1601
AS REQUIRED IN THE GENERAL
ACTS OF ALABAMA, 1975 ACT NO.
919.

JOHN TREADWELL, Clerk

CONFERENCE COMMITTEE

House Conferees _____

SENATE ACTION

DATE: 1/22 2026

RD 1 RFD CYH

This Bill was referred to the Standing Committee
of the Senate on CYH

and was acted upon by such Committee in
session and is by order of the Committee
returned therefrom with a favorable report
w/amend(s) 0 w/sub 0 by a vote of
yeas 9 nays 0 abstain 0
this 24th day of January 20 26
[Signature] Chair

DATE: 1-24 20 25

RF 150 RD 2 CAL

DATE: _____ 20 ____

RE-REFERRED ☐ RE-COMMITTED ☐

Committee _____

I hereby certify that the Resolution as
required in Section C of Act No. 81-889
was adopted and is attached to the Bill,
HB 1601
YEAS 33 NAYS 0

PATRICK HARRIS,
Secretary

FURTHER SENATE ACTION (OVER)

JS 44 (Rev. 04/21)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION

(b) County of Residence of First Listed Plaintiff Virginia
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

J. Evans Bailey, Rushton, Stakely, Johnston & Garrett,
P.A., P.O. Box 270, Montgomery, AL 36101-0270,
334-206-3100

DEFENDANTS

STEVE MARSHALL, in his official capacity as Attorney General of Alabama

County of Residence of First Listed Defendant Montgomery
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question (U.S. Government Not a Party)
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- | | PTF | DEF | | PTF | DEF |
|---|----------------------------|----------------------------|---|----------------------------|----------------------------|
| Citizen of This State | ☐ 1 | ☐ 1 | Incorporated or Principal Place of Business In This State | ☐ 4 | ☐ 4 |
| Citizen of Another State | ☐ 2 | ☐ 2 | Incorporated and Principal Place of Business In Another State | ☐ 5 | ☐ 5 |
| Citizen or Subject of a Foreign Country | ☐ 3 | ☐ 3 | Foreign Nation | ☐ 6 | ☐ 6 |

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Click here for: [Nature of Suit Code Descriptions.](#)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES	
☐ 110 Insurance ☐ 120 Marine ☐ 130 Miller Act ☐ 140 Negotiable Instrument ☐ 150 Recovery of Overpayment & Enforcement of Judgment ☐ 151 Medicare Act ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans) ☐ 153 Recovery of Overpayment of Veteran's Benefits ☐ 160 Stockholders' Suits ☐ 190 Other Contract ☐ 195 Contract Product Liability ☐ 196 Franchise	PERSONAL INJURY ☐ 310 Airplane ☐ 315 Airplane Product Liability ☐ 320 Assault, Libel & Slander ☐ 330 Federal Employers' Liability ☐ 340 Marine ☐ 345 Marine Product Liability ☐ 350 Motor Vehicle ☐ 355 Motor Vehicle Product Liability ☐ 360 Other Personal Injury ☐ 362 Personal Injury - Medical Malpractice	☐ 365 Personal Injury - Product Liability ☐ 367 Health Care/Pharmaceutical Personal Injury Product Liability ☐ 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY ☐ 370 Other Fraud ☐ 371 Truth in Lending ☐ 380 Other Personal Property Damage ☐ 385 Property Damage Product Liability	☐ 625 Drug Related Seizure of Property 21 USC 881 ☐ 690 Other LABOR ☐ 710 Fair Labor Standards Act ☐ 720 Labor/Management Relations ☐ 740 Railway Labor Act ☐ 751 Family and Medical Leave Act ☐ 790 Other Labor Litigation ☐ 791 Employee Retirement Income Security Act IMMIGRATION ☐ 462 Naturalization Application ☐ 465 Other Immigration Actions	☐ 422 Appeal 28 USC 158 ☐ 423 Withdrawal 28 USC 157 INTELLECTUAL PROPERTY RIGHTS ☐ 820 Copyrights ☐ 830 Patent ☐ 835 Patent - Abbreviated New Drug Application ☐ 840 Trademark ☐ 880 Defend Trade Secrets Act of 2016 SOCIAL SECURITY ☐ 861 HIA (1395ff) ☐ 862 Black Lung (923) ☐ 863 DIWC/DIWW (405(g)) ☐ 864 SSID Title XVI ☐ 865 RSI (405(g)) FEDERAL TAX SUITS ☐ 870 Taxes (U.S. Plaintiff or Defendant) ☐ 871 IRS—Third Party 26 USC 7609	☐ 375 False Claims Act ☐ 376 Qui Tam (31 USC 3729(a)) ☐ 400 State Reapportionment ☐ 410 Antitrust ☐ 430 Banks and Banking ☐ 450 Commerce ☐ 460 Deportation ☐ 470 Racketeer Influenced and Corrupt Organizations ☐ 480 Consumer Credit (15 USC 1681 or 1692) ☐ 485 Telephone Consumer Protection Act ☐ 490 Cable/Sat TV ☐ 850 Securities/Commodities/Exchange ☐ 890 Other Statutory Actions ☐ 891 Agricultural Acts ☐ 893 Environmental Matters ☐ 895 Freedom of Information Act ☐ 896 Arbitration ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision ☒ 950 Constitutionality of State Statutes
REAL PROPERTY ☐ 210 Land Condemnation ☐ 220 Foreclosure ☐ 230 Rent Lease & Ejectment ☐ 240 Torts to Land ☐ 245 Tort Product Liability ☐ 290 All Other Real Property	CIVIL RIGHTS ☐ 440 Other Civil Rights ☐ 441 Voting ☐ 442 Employment ☐ 443 Housing/Accommodations ☐ 445 Amer. w/Disabilities - Employment ☐ 446 Amer. w/Disabilities - Other ☐ 448 Education	PRISONER PETITIONS Habeas Corpus: ☐ 463 Alien Detainee ☐ 510 Motions to Vacate Sentence ☐ 530 General ☐ 535 Death Penalty Other: ☐ 540 Mandamus & Other ☐ 550 Civil Rights ☐ 555 Prison Condition ☐ 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN (Place an "X" in One Box Only)

- ☒ 1 Original Proceeding
- ☐ 2 Removed from State Court
- ☐ 3 Remanded from Appellate Court
- ☐ 4 Reinstated or Reopened
- ☐ 5 Transferred from Another District (specify)
- ☐ 6 Multidistrict Litigation - Transfer
- ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
42 USC, Section 1983

Brief description of cause:

Violation of the First - Fourteenth Amendments and Commerce Clause of the U.S. Constitution

VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND \$

CHECK YES only if demanded in complaint:

JURY DEMAND: ☐ Yes ☒ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE

DOCKET NUMBER

DATE

Oct 28, 2026

SIGNATURE OF ATTORNEY OF RECORD

J. E. Bailey

FOR OFFICE USE ONLY

RECEIPT #

AMOUNT

APPLYING IFP

JUDGE

MAG. JUDGE

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I. (a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
 - (b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
 - (c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
- United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
- United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
- Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
- Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).
- V. **Origin.** Place an "X" in one of the seven boxes.
- Original Proceedings. (1) Cases which originate in the United States district courts.
- Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
- Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
- Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
- Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
- Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
- Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
- PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7.** Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.
- VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
- Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
- Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

A

A

ITE TATE I T I T T

Middle

Alabama

COMPUTER & COMMUNICATIONS INDUSTRY
ASSOCIATION

Plaintiff(s)

A

STEVE MARSHALL, in his official capacity as
Attorney General of Alabama

Defendant(s)

SUMMONS IN A CIVIL ACTION

T (Defendant's name and address) STEVE MARSHALL
ATTORNEY GENERAL
501 WASHINGTON AVENUE
MONTGOMERY, ALABAMA 36104

A

T

J. EVANS BAILEY
RUSHTON, STAKELY, JOHNSTON & GARRETT, P.A.
P.O. BOX 270
MONTGOMERY, ALABAMA 36101-0270

I

TREY GRANGER, CLERK OF COURT

Signature of Clerk or Deputy Clerk

A

A

A

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

T (name of individual and title, if any) _____

(date) _____

☐ I (place) _____

(date) _____

☐ I (name) _____

(date) _____

☐ I (name of individual) _____

(name of organization) _____

(date) _____

☐ I _____

☐ (specify):

0.00

I

Server's signature

Printed name and title

Server's address

A