

Brian Willen*
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
31 West 52nd Street, Fifth Floor
New York, New York 10019
Telephone: (212) 999-5800
bwillen@wsgr.com

Deno Himonas (5483)
Elizabeth Sharkey (18655)
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
95 South State Street, Suite 1000
Salt Lake City, Utah 84111
Telephone: (801) 401-8510
dhimonas@wsgr.com
esharkey@wsgr.com

Lauren Gallo White*
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
One Market Plaza, Spear Tower, Suite 3300
San Francisco, California 94105
Telephone: (415) 947-2158
lwhite@wsgr.com

Edward Percarpio*
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
1700 K Street NW, Fifth Floor
Washington, D.C. 20006
Telephone: (202) 973-8800
epercarpio@wsgr.com

**(motions for admission
pro hac vice forthcoming)*

Attorneys for Plaintiff Computer & Communications Industry Association

UNITED STATES DISTRICT COURT
DISTRICT OF UTAH

COMPUTER & COMMUNICATIONS
INDUSTRY ASSOCIATION,

Plaintiff,

vs.

DEREK BROWN, in his official capacity as
Attorney General of Utah; KATHERINE
HASS, in her official capacity as the Director
of the Division of Consumer Protection of the
Utah Department of Commerce,

Defendants.

**COMPLAINT FOR DECLARATORY
AND INJUNCTIVE RELIEF**

Case No. _____

The Computer & Communications Industry Association (“CCIA”) brings this civil action against Defendants for declaratory and injunctive relief and alleges as follows:

INTRODUCTION

1. Utah Senate Bill 142, 2025 Utah Laws Ch. 76 (“S.B. 142” or the “Act”) (Ex. A),¹ imposes a broad censorship regime on mobile apps. In a misguided attempt to protect minors, the Act requires proof of age before anyone with a smartphone or tablet can download a single app. Anyone under 18 must obtain parental consent for every app and 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 Utah’s vague and unworkable set of 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. Our Constitution forbids laws that require businesses to “card” people before they can enter bookstores and community theaters. And the First Amendment prohibits such oppressive laws as much in cyberspace as it does in the physical world. *Packingham v. North Carolina*, 582 U.S. 98, 104 (2017). There is no legitimate purpose for such a law. To the extent any exists, the Act is both fatally overbroad and 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

¹ The Act was enrolled to be codified at Title 13, Chapter 75 of the Utah Code, but was subsequently codified at Title 13, Chapter 76. As a result, the Act mistakenly continues to refer to its sections and subsections as part of Chapter 75, which is now the Franchise Protection Act. For clarity, this Complaint cites to the Act as if these errors have been corrected.

to *remove* parental choice by imposing a one-size-fits-all restriction on the many millions of app store offerings (including books, movies, and games) and app store users, regardless of age and user (or parental) preference.

3. 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 distribute and 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. The Act would prohibit all mobile app stores and app developers from disseminating all but a very select few apps without first complying with onerous age-verification, parental-verification, and parental-consent restrictions that burden the free speech rights of the app stores, app developers, and their users.

4. 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) account creation, (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 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. If a user cannot sufficiently demonstrate they are over 18 years old, the user must link their account to that of a parent or

guardian, meaning an individual with “legal authority” to make decisions on behalf of the minor user, but only after the parent or guardian can prove that they are over 18. §§ 13-76-201(1)(b), 13-76-101(15)-(16).²

- b. *Second*, any user determined to be a minor is forbidden from downloading any mobile app—including mobile newspapers, biblical study apps, the vast majority of educational apps, messaging apps, or games—without first obtaining parental consent for that download, subject to one narrow exception. § 13-76-201(1)(b)(ii)(A)-(B).
- c. *Third*, a verified parent must affirmatively consent to *all* purchases within each 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. § 13-76-201(1)(b)(ii), (1)(c).

5. These requirements have vast and troubling implications for protected speech. Under S.B. 142, if a 14-year-old wants to download the Libby app to borrow an ebook from the Salt Lake City Public Library, she would first have to establish her own age; then she’d 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; finally, she’d have to wait for the parent to provide consent for the app. Similarly, a 17-year-old who wants to purchase a new book to read on his Kindle app would need to jump through all the same hoops and then ask a parent to review and approve his choice. The same is true for apps like ESPN, Wikipedia, Spotify, Audible, Substack, Duolingo, Goodreads, Bible Project, The Book of

² References to “§” are to sections of the Utah Code.

Mormon, Atheism Pocket Debater, TED, Bandcamp, 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 apps provide. Even minors who can successfully link a verified parent account are burdened when their parents are (understandably) too busy to approve each request as it is made.

6. Instead of tailoring its reach to protecting children, the law suppresses speech so broadly that it leaves the First Amendment as collateral damage. Utah has walled off virtually all mobile apps behind a series of verification and consent gates. Indeed, S.B. 142 does nothing to exempt apps that facilitate core political or educational speech; creative or artistic expression; religious instruction and information; or the exchange of ideas, information, and culture. Put bluntly, Utah has “burn[ed] the house to roast the pig.” *Butler v. Michigan*, 352 U.S. 380, 383 (1957).

7. To the contrary, these provisions impermissibly burden app stores and developers in exercising their rights to distribute speech; they burden adults in their right to access and create speech; and they burden the rights of minors to access and create speech without parental approval. For these reasons, the Act is subject to and fails strict scrutiny. But 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 the State’s purported interest in protecting minors online.

8. The Act is a blunt instrument that is simultaneously overbroad in restricting core speech and underinclusive in its narrow focus on mobile apps. It ignores less restrictive alternatives, including existing parental controls, many apps’ existing verification and consent

tools tailored to particular services within those apps, and Utah's targeted obscenity laws, *see* S.B. 287, Utah Code § 78B-3-1001 (2025), while appearing to impose standardless, compelled-speech requirements that dismantle established industry safety frameworks.

9. The Act also violates the Commerce Clause by excessively burdening interstate commerce in relation to the purported local benefit conferred on the State of Utah. The Act forces national platforms to dismantle uniform operations in favor of Utah-specific mandates, forces app stores to comply with an inconsistent patchwork of state rules across the United States, and has the effect of regulating commercial and speech-related activities that occur wholly outside Utah. This compelled fragmentation balkanizes the digital marketplace—impermissibly projecting Utah's idiosyncratic regulatory scheme onto the national economy while failing to provide a constitutionally permissible or effective local shield.

10. The Court should declare S.B. 142 facially unlawful and enjoin its enforcement as to CCIA's app store and developer members.

PARTIES

11. Plaintiff CCIA is an international, non-profit entity 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.

12. Based on S.B. 142'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 users to download apps from third-party developers onto a mobile device.” § 13-76-101(5), (6). Numerous other CCIA members also develop mobile apps that are regulated by the Act.

13. Defendant Derek Brown, the Utah Attorney General, is a resident of Utah and is sued in his official capacity. Defendant Katherine Hass, the Director of the Utah Division of Consumer Protection, is a resident of Utah and is sued in her official capacity.

STANDING

14. CCIA has standing to challenge S.B. 142 on multiple grounds.

15. CCIA has associational standing because (1) some of CCIA’s members have standing, as those members “are subject to the Act and will face injury in the form of liability if they violate its operative provisions;” (2) challenging S.B. 142 is germane to CCIA’s mission; and (3) CCIA members’ individual participation as parties is unnecessary in this purely legal challenge. *NetChoice, LLC v. Reyes*, 748 F. Supp. 3d 1105, 1119 & 1118 n.77 (D. Utah 2024) (collecting cases “brought against similar state laws [that] have reached the same conclusion”); *see also Speech First, Inc. v. Shrum*, 92 F.4th 947, 949 (10th Cir. 2024).

16. *First*, CCIA “ha[s] standing” to bring a pre-enforcement facial challenge against S.B. 142 because the law is “aimed directly at” CCIA’s app store and developer members, “who . . . would have to take significant and costly compliance measures” to implement S.B. 142’s onerous requirements across their technologies. *Reyes*, 748 F. Supp. 3d at 1119, n.78 (quoting *Virginia v. Am. Booksellers Ass’n*, 484 U.S. 383, 392, 108 S. Ct. 636, 642 (1988)). CCIA members operate

app stores and develop apps, and in both capacities (as discussed below), they engage in “constitutionally protected conduct . . . protected by the First Amendment.” *Dias v. City & Cty. of Denver*, 567 F.3d 1169, 1179-80 (10th Cir. 2009).

17. *Second*, in challenging S.B. 142, “the interests at stake are germane to [CCIA’s] purpose.” *Friends of the Earth v. Laidlaw*, 528 U.S. 167, 181 (2000); *Reyes*, 748 F. Supp. 3d at 1119 (finding associational standing when “the interest [an association] aims to protect are central to its organizational purpose”). S.B. 142 imposes unconstitutional restrictions on CCIA members’ ability to speak and facilitate speech through 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.

18. *Third*, CCIA’s claims “do not require the participation of individual members in the lawsuit.” *Reyes*, 748 F. Supp. 3d at 1119 (cleaned up). For example, because the age-verification and parental-consent requirements affect all covered app stores equally, their claims “can be proven without fact-intensive individualized inquiry” into CCIA’s individual members, as is the case here. *Id.* Moreover, “the prospective relief [CCIA] seeks ‘will inure to the benefit of those members of the association actually injured.’” *Id.* (quoting *Warth v. Seldin*, 422 U.S. 490, 515 (1975)).

19. CCIA, through its members operating as both app stores and app developers, also has prudential standing to assert the First Amendment rights of its members’ users—current and prospective. “[B]ecause of the significance of First Amendment rights, the Supreme Court ‘has enunciated other concerns that justify a lessening of prudential limitations on standing.’” *Phelps v. Hamilton*, 122 F.3d 1309, 1326 (10th Cir. 1997) (quoting *Sec’y of State of Md. v. Joseph H.*

Munson Co., 467 U.S. 947, 956 (1984)). “[W]hen there is a danger of chilling free speech . . . [l]itigants . . . are permitted to challenge a statute not because their own rights of free expression are violated, but because of a judicial prediction or assumption that the statute’s very existence may cause others not before the court to refrain from constitutionally protected speech or expression.” *Joseph H. Munson Co.*, 467 U.S. at 956 (quoting *Broadrick v. Oklahoma*, 413 U.S. 601, 612 (1973)).

JURISDICTION & VENUE

20. 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).

21. The Act delegates authority to the Attorney General and the Commerce Division of the Utah Department of Consumer Protection to enforce and to give effect to the Act. *First*, it does so by classifying violations of Subsections 13-76-201(2)(b) and 13-76-202(4)(b) as “deceptive trade practice[s].” § 13-76-401(1); *see also* § 13-11a-4(1)(a).

22. *Second*, S.B. 142 provides that “the [Division of Consumer Protection] shall make rules establishing processes and means by which an app store provider may verify whether an account holder is a minor,” § 13-76-301, obligating the Director to give effect to the Act’s requirements. Further, embedded within the Division’s rulemaking authority is the authority to enforce “violation[s] of the division rules and the laws administered and enforced by it,” § 13-2-5(3), providing the Director with the authority to enforce S.B. 142.

23. *Third*, the delegation to the Attorney General is further evidenced by the Utah Declaratory Judgments Act, which entitles the Attorney General to be heard whenever “a statute . . . is alleged to be invalid.” § 78B-6-403(3) (“If a statute or state franchise or permit is alleged to be invalid, the attorney general shall be served with a copy of the proceeding and be entitled to be heard.”).

24. *Finally*, and relatedly, the Act contains a savings clause providing that “[n]othing in this chapter shall displace any other available remedies or rights authorized under the laws of this state or the United States.” § 13-76-402(4). That includes the Attorney General’s and Director’s above-described authorities to give effect to and enforce the Act’s provisions—including both the provisions enforceable through the Act’s private right of action, § 13-76-401(2), such as sections 13-76-201(2) and 13-76-202(4) (prohibiting app stores and developers from enforcing contracts against minors absent parental consent, from knowingly misrepresenting information in the parental disclosure, and from sharing age verification information except as required by law), and, at a minimum, those that fall outside of it, *see, e.g.*, §§ 13-76-202(4)(c) (prohibiting developers from sharing age category data, including adults’ data, with any person); 13-76-201(1)(d) (requiring app store providers to “provide to a developer, in response to a request authorized under Section 13-76-202 . . . age category data for a user located in the state; and . . . the status of verified parental consent for a minor located in the state.”).

25. This Court has personal jurisdiction over Defendants, because the Utah Attorney General and the Director of the Utah Division of Consumer Protection reside in and/or conduct a substantial portion of their official business in Salt Lake City, Utah.

26. Venue is proper in this district under 28 U.S.C. § 1391(b) because Defendants reside in Utah, and the events giving rise to this civil action occurred in Salt Lake City, Utah.

BACKGROUND & FACTUAL ALLEGATIONS

27. **App Stores Are a Vibrant Forum for Speech.** App stores are digital content stores that allow users to search for, browse, discover, download, and purchase mobile apps and other expressive content. In providing this service, app stores publish and facilitate secure, privacy-protective access to vast quantities of expressive content in every digital media format; they directly facilitate some of the largest and most egalitarian fora for speech and creativity among developers and users.

28. Apps themselves embody, create, and curate diverse fora for speech and interaction. The internet is a vital forum for speech, *Packingham v. North Carolina*, 582 U.S. 98, 104 (2017), and apps facilitate that forum on mobile devices. 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 apps “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). And app stores stand at the threshold of access to those apps.

29. App stores embody and facilitate such diverse fora for speech largely 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.”³ Thus, apps carry out the internet’s promise of “relatively unlimited, low-cost capacity for communication of all kinds.” *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 870 (1997).

30. The vast majority of the most-downloaded apps in member app stores either offer or facilitate free expression.⁴ And as an additional layer of expressive activity and speech, apps embody expressive software design choices, and their operation and maintenance constitute speech acts.

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. **YouVersion Bible App**, which allows people to read or listen to the Bible and share passages and comments with friends in their network;

³ *Small developers on the App Store grew revenue by 71 percent over the past two years*, Apple (May 11, 2023), <https://www.apple.com/newsroom/2023/05/small-developers-on-the-app-store-grew-revenue-by-71-percent-from-2020-2022/>.

⁴ See, e.g., *Top Charts*, Google Play, https://play.google.com/store/apps?hl=en_US (last visited Jan. 28, 2026); *Top Charts - Top Free Apps*, Apple App Store, <https://apps.apple.com/us/charts/iphone/top-free-apps/36> (last visited Jan. 28, 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 Jan. 28, 2026).

- d. **InstaRabbi**, which allows Jews from across the world to ask Torah or Halachic questions and get quick answers in accordance with Orthodox Jewish observance;
- e. **The Book of Mormon**, which allows people to access the Book of Mormon in over 100 different languages, listen to audio narration in several languages, and watch videos of dramatized accounts of the Book of Mormon;
- f. **Spotify**, which allows people to listen to music, podcasts, and audiobooks and share playlists with others;
- g. **NYTimes** and **WSJ Print Edition**, which provide journalism, just as they do in their print newspapers;
- h. **The BYU Cougars app**, which lets fans of Brigham Young University Athletics follow game coverage and news, and view exclusive content;
- i. **BusyKid**, an app that teaches kids financial literacy and independence when they earn money for completing chores;
- j. **Tankee**, a gaming and videosharing service that curates family-friendly content and helps parents ensure that their kids are not watching adult-oriented videos;
- k. **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;
- l. **Waffle Smash**, a game originally designed to help kids with cerebral palsy develop their hand-eye coordination and dexterity;
- m. **StoryPlace**, an online community that allows writers to share original stories;

n. **Smart Kidz Club**, an educational service that helps foster kids' love of reading and math;

o. **Sudoku Master!**, which allows people to choose among 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, YouTube, Goodreads, 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. 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 and youtube.com) or through non-mobile apps that can be downloaded on a Smart TV. The Act's impact is thus to make accessing speech and information more difficult and disjointed.

34. **Apps 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, all of CCIA’s app store members 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.

35. Every app store, on information and belief, engages 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 new *de facto* age rating requirements potentially 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

36. 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 Jan. 28, 2026).

⁶ Age ratings values and definitions, Apple, <https://developer.apple.com/help/app-store-connect/reference/age-ratings-values-and-definitions/> (last visited Jan. 28, 2026).

⁷ Design safe and age-appropriate experiences for your apps and games, Apple, <https://developer.apple.com/kids/> (last visited Jan. 28, 2026).

37. For apps directed towards younger audiences, CCIA’s app store members also impose and enforce different and 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.

38. 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.

39. 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 to set up controls on their children’s accounts.⁸ 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.⁹ The Apple App Store similarly allows parents to set age-related restrictions for content, prevent their children from installing apps and making in-app purchases in apps, prevent children from deleting parental-monitoring apps, restrict app downloads and games, and manage their child’s privacy settings.¹⁰ Additionally, Amazon’s Parent Dashboard allows parents to monitor the apps their children are interacting with, set daily limits or restrict

⁸ *How to Set Up Parental Controls on Google Play*, Google Play, <https://support.google.com/googleplay/answer/1075738?hl=en> (last visited Jan. 28, 2026).

⁹ *Id.*

¹⁰ *Use Parental Controls on Your Child’s iPhone or iPad*, Apple, <https://support.apple.com/en-us/105121> (last visited Jan. 28, 2026).

their children’s use at certain times of day, and restrict access to content that parents might find inappropriate for their child.¹¹ 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 500 thousand downloads in the Google Play Store.

40. By crafting, publishing, and enforcing content policies and providing tools to allow parents to limit access to app content, app stores actively engage in expressive activities, selecting which apps to publish, to whom, when, and how. This expressive conduct is protected by the First Amendment. *Moody v. NetChoice*, 603 U.S. 707, 731 (2024).

41. 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 S.B. 142’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.

UTAH S.B. 142: RELEVANT PROVISIONS

42. **Age Verification, Parental Tethering, and Legal Authority Verification to Enable Parental Consent (“Account Restrictions”).** Under the Act, whenever an individual

¹¹ *Amazon Parent Dashboard*, Amazon.com, <https://www.amazon.com/parentdashboard/intro> (last visited Jan. 28, 2026).

creates an account with an app store, the app store must “verify the individual’s age category using . . . commercially available methods that are reasonably designed to ensure accuracy,” or else comply with rules to be promulgated by the Division of Consumer Protection. § 13-76-201(1)(a). Individuals are divided into four age categories: younger than 13 (“child”); at least 13 and younger than 16 (“younger teenager”); at least 16 and younger than 18 (“older teenager”); and at least 18 (“adult”). § 13-76-101(1).

43. If the user is determined to be under 18, the Act requires the account be affiliated with an account belonging to a parent or guardian. § 13-76-201(1)(b). To be affiliated, the “parent” must have “legal authority to make decisions on behalf of the minor,” meaning they must be an individual with a parent-child relationship under Utah law, a legal guardian, or an individual with legal custody. § 13-76-101(15). The app store must verify the parent or guardian’s account was “established by an individual who the app store provider has determined is at least 18 years old through the app store provider’s age verification methods.” § 13-76-101(16)(a).

44. App developers are required to verify the age category assigned to each user and, for minors, whether parental consent has been obtained, based on information provided by the app store. § 13-76-202(1)(a). Developers must then “use age category data received from an app store provider” to “enforce any developer-created age-related restrictions,” “ensure compliance with applicable laws and regulations,” and “implement any developer-created safety-related features or defaults.” § 13-76-202(1)(c). However, the Act *also* provides that developers must “use the lowest age category indicated by” either the age verification data provided by the app store *or age data independently collected by the developer* when implementing any developer-created safety-related features or defaults. § 13-76-202(3).

45. The Act does not provide any guidance on how to verify age or determine whether an adult has the requisite legal authority over the minor to be affiliated.

46. The choice of using *either* “commercially available methods that are reasonably designed to ensure accuracy” *or* a “method or process that complies with rules made by” the Division in the age-verification provisions does not alter which app stores or apps the Act covers. Nor does it alleviate the unconstitutional burdens. Rather, on the one hand, the law provides that app stores may rely on methods “reasonably designed to ensure accuracy.” Alternatively, app stores might attempt to comply with rules, to be promulgated by the Division without any guidance from the legislature, purportedly creating a standard for handling the rapidly evolving, technologically challenging issue of age verification. This choice does not resolve the uncertainty for app stores, nor does it serve any purported governmental interests.

47. Nor does the purported availability of alternative methods of compliance 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—*except for* apps that are operated by, or in partnership with, a government entity, nonprofit, or authorized emergency service provider and provide direct access to emergency services, and which meet certain data collection and technical requirements. § 13-76-404(4). The statute has no provision that would permit parents to opt out of or streamline this onerous consent requirement. To the contrary, the Act requires app stores to obtain verifiable parental consent before allowing a minor to download or purchase an

app or make an in-app purchase. § 13-76-201(1)(b)(ii). And because verifiable parental consent requires providing a disclosure that includes information *about the specific app being consented to*, § 13-76-101(17), (19), 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 consent from the parent account on an ongoing basis *every single time* a minor wants to make an in-app purchase. § 13-76-201(1)(b)(ii)(C). Further, S.B. 142 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 the content elements that led to that rating. §§ 13-76-101(7) (“[c]ontent description”); 13-76-101(17) (“[p]arental consent disclosure”), 13-76-101(18) (“[s]ignificant change”), 13-76-202(1)(b). When such a change is made, S.B. 142 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. §§ 13-76-202(1)(b), 13-76-101(18).

50. Age Rating 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, “if the app store provider has” an age rating or content description for an app or in-app purchase, the Act requires the app store to disclose that age rating or content description in order to obtain “verifiable parental consent.” §§ 13-76-201(1)(b)(ii); 13-76-101(17), (19). The Act also holds both developers and app stores liable for “knowingly misrepresent[ing]” any information in that disclosure. §§ 13-

76-201(2)(b), 13-76-202(4)(b). At the same time, a developer is protected by a safe harbor from the risk of liability for “knowingly misrepresent[ing]” an age rating, but only 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. §§ 13-76-402(2), 13-76-101(1). Similarly, developers are required to request age verification data collected by app stores *using the State’s age categories*, § 13-76-201(1)(d), and use that data to enforce any developer-created age-related restrictions and implement any safety-related features or defaults. § 13-76-202(1)(c)(i), (iii).

51. These provisions thus 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 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. § 13-76-101(17), (19). The lack of clarity regarding whether this is the proper interpretation of S.B. 142 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; adds new monetization features (including in-app purchases or advertisements); changes the categories of data collected, stored, or shared; or “materially changes” the app’s functionality or user experience. §§ 13-76-101(18), 13-76-202(1)(b).

EFFECTS OF S.B. 142’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. 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. App stores enjoy First Amendment protection both when they disseminate and make available speech, *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 557 (2011), and when they “present[] a curated compilation of speech originally created by others.” *Moody*, 603 U.S. at 728.

54. The verification and consent requirements impose direct burdens on app stores’ freedom to disseminate protected speech. The requirements insert a barrier between speech disseminated through the app stores and the audience of that speech—blocking many users entirely. 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 v. Entm’t Merchs. Ass’n*, 564 U.S. 786, 795 n.3 (2011). For example, a 14-year-old cannot purchase the audiobook version of *The Giver* from Audible until her parent or guardian approves the purchase. If her parent or guardian is too busy or refuses to approve the request, or cannot adequately prove legal authority, the minor would be blocked entirely from listening to the John Newbery Medal-winning novel.

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); *NetChoice v. Fitch*, 134 F.4th 799, 807 (5th Cir. 2025). Although the Act is purportedly about protecting children, age verification 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.¹² Further, the Federal Reserve reports that, in 2023,

¹² 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>.

approximately 18% of adults in the United States did not have a credit card.¹³ Additionally, “[c]hildren generally don’t have government IDs[,]”¹⁴ and often do not have credit cards, either.¹⁵

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. All age-verification methods also risk excluding some members of 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 S.B. 142 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), S.B. 142’s all-encompassing sweep virtually guarantees that all smartphone users in Utah will have to submit to age verification to download a single app from an app store. And unlike most other age-verification laws, S.B. 142 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

¹³ Report on the Economic Well-Being of U.S. Households in 2023, U.S. Federal Reserve (May 2024), www.federalreserve.gov/publications/files/2023-report-economic-well-being-us-households-202405.pdf (last visited Jan. 28, 2026).

¹⁴ Shoshana Weissmann, *Kids Don’t Have IDs and Age-Estimation Tech Is Frequently Very Wrong*, Techdirt (May 23, 2025, 11:02 AM), <https://www.techdirt.com/2025/05/23/kids-dont-have-ids-and-age-estimation-tech-is-frequently-very-wrong/>; Jake Taylor, *Fewer Utah Teens Choosing to Get Driver Licenses*, KUTV (Mar. 7, 2024), <https://kutv.com/news/local/fewer-utah-teens-choosing-to-get-driver-licenses-ntsb-uber-eats-rideshare-apps-time-expensive-prices-friend-influence>.

¹⁵ See Barri Segal, *Poll: 8 Percent of U.S. Parents Have Children with Credit Cards*, creditcards.com (Mar. 24, 2019), <https://www.creditcards.com/statistics/kids-and-credit-cards-poll/>.

purported parent does in fact have “legal authority to make decisions on behalf of the minor.” § 13-76-101(15).

60. These verification requirements then feed into the Act’s unnecessarily onerous parental consent requirement any time a minor wants to download or purchase almost any mobile app, make any 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 verification and consent requirements of S.B. 142 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. § 13-76-201(1)(d). Developers are then required to maintain the security of the data received from app stores during this process in order to avoid improperly sharing users’ age category data. § 13-76-202(4)(c). 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 swathes of developers from disseminating—and huge numbers of users from accessing—lawful speech. S.B. 142 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 S.B. 142, 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 Utah 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 Utah.

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. §§ 13-76-101(17), (19); 13-76-201(1)(b)(ii). 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 Utah 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) (emphasis added) (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 that 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. S.B. 142’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. 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 S.B. 142’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 LLC v. Elenis*, 600 U.S. 570, 586-87 (2023).

68. The Act requires both app stores and developers to identify users’ ages within four categories: child, younger teenager, teenager, and adult. § 13-76-101(1). The gradations between child and younger teenager, younger teenager and teenager, and teenager and adult require relatively high degrees of specificity, and the success of the Act is in large part dependent on accurate categorization (within the State’s, or a private litigant’s, judgment of accuracy). These do not 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 “young teens” versus “teens.”

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. § 13-76-202(4). And if an app store provider “has” an age rating for an app or in-app purchase, it must be included in the parental consent disclosure. § 13-76-101(17), (19). A developer is protected from liability for any “knowing misrepresentation” in the parental disclosure if, “[f]or purposes of setting the age category of an app and providing content description disclosures to an app store provider,” the developer “uses widely adopted industry standards to determine” the “age category.” § 13-76-402(2). The term “age category” specifically means ***Utah’s chosen age ratings***. 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 provide those categories and resulting content descriptions to app stores. § 13-76-101(1). Further bolstering this requirement, the Act obligates developers to request age verification data, collected by app stores *in line with the State’s age categories*, § 13-76-201(1)(d), and use that data to enforce any developer-created age-related restrictions and implement any safety-related features or defaults, such as age ratings for in-app purchases. § 13-76-202(1)(c)(i), (iii).

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 to app stores, app stores will be compelled to disclose those ratings 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. §§ 13-76-201(b)(ii)–(c), 13-76-101(17).

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 (Book People II)*, 91 F.4th 318, 329-330 & 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), *aff’d sub nom. Brown v. Entm’t Merchs. Ass’n*, 564 U.S. 786 (2011) (“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.”).

72. These age-rating 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. **Counts I and II:** constitutional challenges to the verification and consent requirements and their associated violation provisions, brought facially with respect to the provisions affecting app stores, and as applied to CCIA's app store and developer members;
- b. **Counts III and IV:** constitutional challenges to the age-rating and disclosure requirements and associated violation provisions brought facially and as applied to CCIA members in their capacities as app developers and app stores;
- c. **Count V:** a vagueness challenge to the age-rating and disclosure requirements and associated violation provisions;
- d. **Count VI:** a vagueness challenge to the notice of significant changes provision;
- e. **Count VII:** a commerce clause challenge as to S.B. 142 as a whole; and
- f. **Counts VIII & IX:** requests for equitable and declaratory relief related to the above claims.

74. For the First Amendment claims, the facial challenge standard asks whether “a substantial number of [S.B. 142’s] applications are unconstitutional, judged in relation to the statute’s plainly legitimate sweep.” *Moody*, 603 U.S. at 723 (citation omitted). S.B. 142 has *no* constitutional applications to app stores and developers. 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)). S.B. 142’s indiscriminate barriers to access and compelled speech mandates impose burdens that fall uniformly across all app stores and developers whose speech

can no longer be freely accessed, and who are forced to engage in and communicate the State's speech.

75. For CCIA's First and Fourteenth Amendment vagueness claims, a facial vagueness challenge is proper because "the challenged law would be vague in the vast majority of its applications[.]" *Doctor John's, Inc. v. City of Roy*, 465 F.3d 1150, 1157 (10th Cir. 2006). "To mount a facial vagueness challenge," CCIA need only show that "that the potential chilling effect on protected expression is both real and substantial." *Jordan v. Pugh*, 425 F.3d 820, 828 (10th Cir. 2005) (citation omitted). Thus, facial "[v]agueness and overbreadth challenges are similar." *United States v. Gaudreau*, 860 F.2d 357, 360 (10th Cir. 1988); *see Kolender v. Lawson*, 461 U.S. 352, 358 n.8 (1983) (similar).

76. 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
(App Stores: Age-verification and parental-consent requirements, Utah Code §§ 13-76-201(1)(a), 13-76-201(1)(b), 13-76-201(1)(c)(ii), 13-76-201(1)(d), 13-76-201(1)(e), 13-76-201(2)(a); 13-76-301)

77. Plaintiff incorporates all prior paragraphs as if fully set forth herein.

78. **S.B. 142 Burdens the Dissemination, Curation, and Access to Protected Speech.** The Act requires app stores to verify the age of every user before they will be permitted access to their services, and then force any minor user to tether their account to a verified parent or guardian and obtain consent before they can download or purchase almost any app. These provisions burden app stores', app developers', and users' rights to free expression under the First

Amendment. Because the Act functions as a barrier to both adults' and minors' access to protected speech, S.B. 142 triggers and fails strict scrutiny.

79. Countless apps available on CCIA members' services provide constitutionally protected speech to both adults and minors, as well as opportunities for app users to create and disseminate their own pure speech. 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, app stores present a curated compilation of speech originally created by others. S.B. 142's verification and consent requirements unequivocally regulate and burden speech, age-gating the primary gateway to the internet on mobile devices. Those gates open only if the individual first passes the app store's age-verification and, if the user is a minor, the parental-identity verification, parental-tethering, and parental-consent requirements imposed by the Act.

80. For people who don't 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. 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.

81. 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 parent has "legal authority" over that minor. §§ 13-76-201(1)(b)(i), 13-76-101(15)-(16). Then, of course, the parent must decide whether to authorize the minor's download or purchase of the app. § 13-76-201(1)(b)(ii)(A)-(B). 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), § 13-76-201(b)(ii)(C), and every time the app makes a so-called “significant change” to its terms of service or privacy policy, § 13-76-201(1)(c). 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[.]”).

82. S.B. 142’s Age-Verification and Parental-Consent Regime Operates as a Prior Restraint, Triggering Strict Scrutiny. S.B. 142 operates as a prior restraint on speech by forcing private actors to interpose and enforce the State’s access gates on all manner of protected speech. The Act’s restraints burden speech on every level of the app environment, including: (1) all would-be app users’ access to protected speech; (2) minors’ ability to produce and receive protected speech; (3) developers’ ability to create and distribute protected speech; and (4) app stores’ ability to curate and publish protected speech to all audiences.

83. S.B. 142 impermissibly enlists app stores to carry out a vast censorship scheme on behalf of the State. *First*, app stores are forced to verify the age of every single user via invasive age verification procedures before allowing adults 18 and older access to a vast array of protected speech or, for minor, requiring minor users to tether their accounts to a parental account. *Second*, the Act forces 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 app

stores to impose these restrictions, which will deter adults and minors alike from accessing apps they otherwise would.

84. In widening S.B. 142's aperture to swallow up so much speech, the State's targeting of protected speech is not merely incidental—it is direct.

85. **The Verification and Consent Requirements Fail Any Form of Heightened Scrutiny.** Each of these types of effects—prior restraints and broad impacts on speech—subjects the Act to strict scrutiny. But Utah could not satisfy its burden even under intermediate scrutiny because 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 S.B. 287, Utah Code § 78B-3-1001 (2025); and it is underinclusive by failing to impose any gates around web-based or non-mobile analogs. 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.

86. **The Verification and Consent Requirements Are Overbroad.** S.B. 142 imposes verification and consent as gates that bar access to every single 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.

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

88. The State's practical prohibition of blanket parental consent underscores the tailoring problem and unnecessarily burdens parents. As written, S.B. 142 requires app stores and

parents to wade through several layers of consent on an app-by-app, and purchase-by-purchase basis. It is unclear how 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 furthers 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, 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 downloading books, videos, or music within them.

89. 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.

90. All major app stores provide more robust parental control offerings than S.B. 142 requires, should parents decide that it is best for them to employ. 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.¹⁶ The Google Play Store offers

¹⁶ *Set Parental Controls for In-App Purchases*, Amazon.com, <https://www.amazon.com/gp/help/customer/display.html?nodeId=GB8P5MQSYFYHPCQ5> (last visited Jan. 28, 2026).

parents the same functionality through its Family Link feature,¹⁷ as does the Apple App Store through Screen Time.¹⁸

91. 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 categories. Apple, for instance, allows parents to block music, videos, or podcasts that contain explicit content and to prevent books, movies, TV shows, and apps with specific content ratings.¹⁹ 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.²⁰ The Amazon Appstore will “reject[] or suppress[]” apps that contain content that would not be considered “family-friendly.”²¹

92. Individual apps 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.²²

¹⁷ *How To Set Up Parental Controls on Google Play*, Google, <https://support.google.com/googleplay/answer/1075738?hl=en> (last visited Jan. 28, 2026).

¹⁸ *Use Parental Controls on Your Child’s iPhone or iPad*, Apple, <https://support.apple.com/en-us/105121> (last visited Jan. 28, 2026).

¹⁹ *Id.*

²⁰ *How To Set Up Parental Controls on Google Play*, Google, <https://support.google.com/googleplay/answer/1075738?hl=en> (last visited Jan. 28, 2026).

²¹ *Amazon Appstore Content Policy*, Amazon.com, <https://developer.amazon.com/docs/policy-center/understanding-content-policy.html> (last visited Jan. 28, 2026).

²² See, e.g., *Supervised experiences for pre-teens – Understand your choices as a family*, YouTube, <https://support.google.com/youtube/answer/10315420> (last visited Jan. 28, 2026); *Parental Controls on Netflix*, Netflix, <https://help.netflix.com/en/node/264> (last visited Jan. 28, 2026).

93. Instead of empowering parents to use these tools where they believe them appropriate for their families, the State now legally obligates parents to use them, and in doing so subjects *all* app store users to an invasive identity verification process.

94. 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 S.B. 142, the State forces every parent to review and approve every app download and every in-app transaction for every app available (except the limited content-based exception discussed above).

95. Utah also has at least one existing law that is targeted to preventing minors from accessing obscenity online. *See* S.B. 287, Utah Code § 78B-3-1001 (2025). Utah also has longstanding protections for minors who enter into contracts, permitting them to disaffirm contracts before reaching majority or a reasonable time after. Utah Code Ann. § 15-2-2 (1999). In light of these preexisting regulations, other state law, and voluntary protective features, S.B. 142 goes far beyond any asserted state interest in protecting minors online.

96. **The Act Is Also Underinclusive.** In addition to its overbreadth issues, S.B. 142 is wildly underinclusive. The Act targets only apps and app stores on “mobile device[s],” §§ 13-76-101(4), 13-76-101(13), and does nothing whatsoever to prevent minors from accessing the exact same content via a web browser or non-mobile app—or in a brick-and-mortar location.

97. Many mobile apps have an identical web-based analog for their content also accessible on mobile devices. Minors can therefore entirely skirt the verification and consent regime and access the content the State seeks to gatekeep from any web browser on their phone or

other device. Moreover, many mobile apps, such as YouTube, Hulu, or Prime Video, have identical counterparts on smart TVs—non-mobile devices that the Act also does not regulate.

98. By overregulating mobile apps while ignoring similar or identical content available via web browsers, smart TV apps, and other media, S.B. 142 simultaneously imposes tremendous burdens on speech while failing to serve its own purported state interests.

99. For these reasons, S.B. 142 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 II
42 U.S.C. § 1983; Ex Parte Young

**VIOLATION OF THE FIRST AMENDMENT, AS INCORPORATED AGAINST THE
STATES THROUGH THE FOURTEENTH AMENDMENT**

(App Developers: Age-verification and parental-consent requirements, Utah Code §§ 13-76-201(1)(a), 13-76-201(1)(b), 13-76-201(1)(d), 13-76-201(1)(e), 13-76-201(2)(a), 13-76-202(1), 13-76-202(4)(a); § 13-76-301)

100. CCIA incorporates all prior paragraphs as though fully set forth herein.

101. **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.

102. These apps apply and enforce their own content and policy guidelines and, in some cases, offer curated experiences for younger or more sensitive audiences.

103. 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.

104. S.B. 142’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.

105. Further, S.B. 142 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: (i) the age category of users located in [Utah]; and (ii) for a minor account, whether verifiable parental consent has been obtained[.]” § 13-76-202(1)(a). This creates yet another burden on CCIA member developers because they must verify this information before permitting their users to access their apps and content (including every in-app purchase).

106. 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 it constitutes a prior-restraint on speech. Further, the developer-verification provision (§ 13-76-202(1)(a)) 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.

107. The Verification, Consent, and Developer-Verification Requirements Are Not Narrowly Tailored. In subjecting all mobile apps, with a single narrow, content-based exception, to S.B. 142’s verification, consent, and developer-verification requirements, the Act sweeps in

huge swaths of protected speech, rather than creating a narrowly tailored solution, as the First Amendment demands.

108. The Act also disregards clear less restrictive alternatives and existing parental controls at both the app store and individual app level that provide the exact functionalities the law requires, and more. 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* §§ 13-76-101(17), (19); 13-76-201(1)(b)(ii), 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*. That is both burdensome and unnecessary.

109. 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).

110. For these reasons, S.B. 142 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 III

42 U.S.C. § 1983; Ex Parte Young

VIOLATION OF THE FIRST AMENDMENT, AS INCORPORATED AGAINST THE STATES THROUGH THE FOURTEENTH AMENDMENT

**(App Developers: Age rating requirements, Utah Code §§ 13-76-202(1)(b), 13-76-202(1)(c),
13-76-202(3), 13-76-202(4)(b)), 13-76-402(2))**

111. CCIA incorporates all prior paragraphs as though fully set forth herein.

112. 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 four specified categories. 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 or elements that led to that rating.” §§ 13-76-202(1)(b); 13-76-101(7), (18). Developers may be held liable for knowingly misrepresenting any information in the parental consent disclosure, including age ratings. § 13-76-202(4)(b).

113. To the extent the Act is read to require app developers to age-rate their apps and in-app purchases, 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.

114. At the app store level, while CCIA’s app store members currently implement their own content-ratings at the app level, S.B. 142 could be read to, in practice, require developers to rate their apps in line with the Act’s age categories and provide 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. § 13-76-202(4)(b). But “[f]or purposes of setting *the age category* of an app and providing content description disclosures to an app store provider,” a developer has complied with its obligation not to knowingly misrepresent any information in the parental consent disclosure “if the developer . . . uses widely adopted industry standards to determine . . . the app’s *age category*; and the *content description* disclosures,” § 13-76-402(2) (emphases added)). This could be interpreted to mean that app developers are only entitled to this safe harbor if they use the State’s proscribed four-

tiered age rating scheme. *See* § 13-76-101(1). 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 S.B. 142’s prescribed age categories.

115. At the level of apps themselves, the Act also requires developers to “use *age category* data received from an app store provider,” to “enforce any developer-created age-related restrictions,” § 13-76-202(1)(c)(i) (emphasis added). 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.

116. This age-rating 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 age-rating 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 forego their existing rating regimes in favor of S.B. 142’s, thereby infringing upon their editorial and curatorial rights. To the extent Utah intends to adopt this interpretation of S.B. 142, Utah seeks to overwrite the existing content rating systems used by apps that disseminate third-party speech (e.g., YouTube,²³ Prime Video) with its own state-mandated rating system.

²³ 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).

117. **The Age-Rating 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,” *KT&G Corp. v. AG of Okla.*, 535 F.3d 1114, 1137 n.14 (10th Cir. 2008) (quoting *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n*, 447 U.S. 557, 561 (1980)), and it “does [] more than propose a commercial transaction,” *United States v. United Foods*, 533 U.S. 405, 409 (2001).

118. *Second*, even regulations compelling commercial speech receive at least intermediate scrutiny. *Nat'l Inst. of Fam. & Life Advoc. v. Becerra (NIFLA)*, 585 U.S. 755, 773 (2018); *accord Free Speech Coal. v. Paxton*, 95 F.4th 263, 283 (5th Cir. 2024) (“NIFLA suggests that compelled speech must survive, *at minimum*, intermediate scrutiny”), *aff'd*, 606 U.S. 461 (2025). To the extent S.B. 142 compels age rating, 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 S.B. 142 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. 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 II*, 91 F.4th at 340 (holding that state-mandated content ratings for

YouTube content rating, YouTube, <https://support.google.com/youtube/answer/146399?hl=en> (last visited Jan. 28, 2026).

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).

119. *Third*, if S.B. 142 is read to require age rating and disclosure of those ratings, that requirement is unduly burdensome, *NIFLA*, 585 U.S. at 776, because app stores and 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. Moreover, existing industry standards, such as the ESRB guidelines, are at odds with the Act’s age categories.

120. **The Age-Rating Provisions Would Fail Under Any Level of Scrutiny.** Such an age-rating 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, *see Free Speech Coal.*, 606 U.S. at 477; 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.

121. 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 S.B. 142’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.

122. 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.

123. Accordingly, to the extent S.B. 142 is properly interpreted to require developers to rate their apps and in-app purchases in compliance with the Act's age categories, that age-rating 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.

124. For these reasons, S.B. 142 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 IV

42 U.S.C. § 1983; Ex Parte Young

VIOLATION OF THE FIRST AMENDMENT, AS INCORPORATED AGAINST THE STATES THROUGH THE FOURTEENTH AMENDMENT

(App Stores: Age rating disclosure requirement, Utah Code §§ 13-76-201(1)(b), 13-76-201(1)(c), 13-76-201(2)(b))

125. CCIA incorporates all prior paragraphs as though fully set forth herein.

126. The Act requires that if an app store has an age rating for an app or in-app purchase, it must disclose that age rating as a precondition to procuring parental consent for app downloads,

purchases, and in-app purchases. §§ 13-76-201(1)(b)(ii), 13-76-101(7). Thus, to the extent the Act in practice requires developers to provide app stores with *the Act's* required age ratings to avoid liability (discussed *supra* Count III), it also requires that app stores disclose *the Act's* ratings as a precondition to procuring parental consent for app downloads and in-app purchases.

127. The Act further subjects app stores to liability for “knowingly misrepresent[ing]” the age rating or content elements that led to the rating. § 13-76-201(2)(b).

128. The Age-Rating Disclosure Requirement Would Be Compelled Speech Subject to Strict Scrutiny. Were it not for S.B. 142, CCIA’s app store members *would not* disclose S.B. 142’s arbitrary age ratings in any context. Nor, on information and belief, do app stores disclose an age rating in the manner potentially required by the Act. Additionally, app stores do not disclose age ratings for in-app purchases, or whenever developers make a significant change to their apps’ terms of service. But to the extent the Act requires such disclosures, it thus significantly expands the instances and alters the manner in which app stores will have to display age ratings.

129. As with app developers, forcing app stores to display an age rating that they otherwise would not display and that they do not themselves necessarily condone is a content-based compulsion of speech. Because the speech that S.B. 142 would require app stores to endorse—i.e., opinions about the age appropriateness of content—is neither factual nor uncontroversial, it is non-commercial and therefore subject to strict scrutiny. *See Free Speech Coal.*, 95 F.4th at 279; *Book People II*, 91 F.4th at 340; *Video Software Dealers Ass’n*, 556 F.3d at 953; *Entm’t Software Ass’n v. Blagojevich*, 469 F.3d at 652; *Riley*, 487 U.S. at 795. Further, to the extent the Act requires disclosure of the Act’s age rating, that provision also infringes upon app stores’ editorial and curatorial rights, *Moody*, 603 U.S. at 728, by forcing app stores to choose

between either subordinating their existing and robust age-rating regimes in favor of S.B. 142's, or displaying both their own age rating and the Act's (as provided to the app store by a developer)—potentially resulting in conflicting information in the parental disclosure and exposing the app store to liability.

130. The Disclosure Requirement Would Fail Even Under Heightened Scrutiny.

The disclosure requirement's lack of narrow tailoring and overbreadth is immediately apparent in its direct conflict with app stores' existing age-rating structures.

131. Not only would S.B. 142's requirement that app stores display the Act's age ratings be content-based compelled speech, it would also be wholly unnecessary because app stores already display age ratings for apps. There is no need for a mandate where age rating is already done on a voluntary basis and pursuant to age categories even more granular and informative for parents than those required by the Act. Thus, the mandated disclosure of S.B. 142's arbitrary and broader age-rating categories would *reduce* the information that parents receive about the age appropriateness of a given app from the status quo. Such a rigid mandate also highlights clearly less restrictive alternatives, including, at minimum, a more reasonable interpretation of the law that does not expose app stores to liability for using their existing age ratings in all contexts in lieu of S.B. 142's vague and directionless regime; or a law that required use of Utah's rating scheme only for content it cares about. Such alternatives would not hamper the State's purported goal of providing parents with visibility into apps' age-appropriateness, and would avoid burdensome compliance costs, issues of unconstitutional vagueness (discussed *infra* Count V), and encroachment on protected editorial rights.

132. For these reasons, S.B. 142 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, Utah Code §§ 13-76-201(1)(b)(ii), 13-76-201(1)(c), 13-76-201(2)(b), 13-76-202(1)(b)-(c), 13-76-202(3), 13-76-202(4)(b); 13-76-402(2))

133. CCIA incorporates all prior paragraphs as though fully set forth herein.

134. 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.

135. “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, S.B. 142 makes it impossible for app developers to ascertain their obligations under the law.

136. S.B. 142 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 § 13-76-101(1), but it simultaneously could be read to impose liability for failure to do so. On the one hand, S.B. 142 holds *developers* liable for “knowingly misrepresent[ing] any information in the parental consent disclosure,” § 13-76-202(4)(b), including age ratings. On the other hand, the Act requires that *app stores*, not developers, provide the parental consent disclosure. §§ 13-76-201(1)(b), (c), 13-76-

101(19). 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 the app store provider has” such an age rating or content description, § 13-76-101(17), (19), it simultaneously provides that developers are entitled to a safe harbor if they, “[f]or purposes of setting the age category of an app and providing content description disclosures to an app store provider,” use “widely adopted industry standards to determine” the app’s “age category” and “the content description disclosures,” and “appl[y] those standards consistently and in good faith,” § 13-76-402. 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.

137. Further, as discussed *supra* ¶ 35, app stores have existing, voluntary age-rating standards for apps that directly conflict with S.B. 142’s age categories. The Act, which requires app stores to disclose age ratings they “ha[ve]” as a precondition to procuring parental consent, § 13-76-101(17), (19), 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 app stores “ha[ve]” those ratings. But the Act simultaneously 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. App stores will thus sometimes “ha[ve]” two conflicting age ratings for a particular app, 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 men of common intelligence must necessarily guess at [their] meaning and differ as to [their] application[.]” *Brennan v. OSHRC*, 505 F.2d 869, 872 (10th Cir. 1974).

138. In addition to the incomprehensible obligations imposed on developers in the context of the parental consent disclosure, the Act also requires developers to “use age category data received from an app store provider” to “enforce any developer-created age-related restrictions” and “implement any developer-created safety-related features or defaults,” § 13-76-202(1)(c), such as app and in-app content age ratings. However, S.B. 142 *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. § 13-76-202(3). 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.

139. 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. § 13-76-101(1). 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* §§ 13-76-402(2)(a); 13-76-101(1).

140. These amorphous standards also raise concerns about disparate enforcement, especially given that Utah has made clear that it is concerned about protecting minors from certain types of content over others.

141. This lack of guidance, combined with the imposition of liability, threatens to undermine the age rating and disclosure system imposed by S.B. 142. 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, §§ 13-76-201(1)(b), 13-76-101(17), 13-76-101(7), 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 children²⁴ 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.)

142. 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

²⁴ *Kids*, Prime Video, <https://www.amazon.com/gp/video/kids> (last visited Jan. 28, 2026).

consent, and may lead parents to deny access to apps that would otherwise be appropriate for children due to an over-inflated age rating.

143. For these reasons, S.B. 142 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 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, Utah Code § 13-76-202(1)(b))

144. CCIA incorporates all prior paragraphs as though fully set forth herein.

145. The Act further requires developers to “notify app store providers of a significant change to the app.” § 13-76-202(1)(b). A change is significant if it is “a material modification to an app’s terms of service or privacy policy” that “changes the categories of data collected, stored, or shared,” “alters the app’s age rating or content descriptions,” adds “new monetization features” including “in-app purchases” or “advertisements,” or “materially changes” the app’s “functionality” or “user experience.” § 13-76-101(18).

146. 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 song, book, movie, or item added to a repository like Apple Music, Audible, or Prime Video, or new content monetized on YouTube using ContentID. Similarly, the “advertisements” presented in apps constantly change—so does each new ad trigger a new notice requirement? The Act’s lack of guidance on these points and others means that developers “must necessarily guess at its meaning and differ as to its application[.]” *Brennan*, 505 F.2d 872.

147. 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, §§ 13-76-201(1)(c), (2)(a)-(b), this provision threatens to impose severe restraints on developers' and users' speech.

148. 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).

149. 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

150. S.B. 142 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 VII
42 U.S.C. § 1983; Ex Parte Young
VIOLATION OF THE COMMERCE CLAUSE OF THE UNITED STATES
CONSTITUTION

151. CCIA incorporates all prior paragraphs as though fully set forth herein.

152. S.B. 142 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 Utah. It is also likely to subject businesses to inconsistent state regulations.

153. S.B. 142 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 Utah'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.

154. S.B. 142 also burdens interstate commerce by forcing app stores to comply with an inconsistent patchwork of state rules. For example, S.B. 142 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 S.B. 142, without regard to any different or conflicting age ratings app developers have adopted or might be required to adopt in other states.

155. The Utah 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 the same content that exists on apps from their website counterparts. Therefore, even if Utah's interest was deemed sufficiently local, S.B. 142's drastic impositions on interstate and online commerce far outweigh what little the Act does to further that purpose.

156. S.B. 142 also violates the Commerce Clause because it regulates extraterritorially in violation of *Healy v. Beer Inst., Inc.*, 491 U.S. 324, 336 (1989). For the same reasons that S.B. 142 burdens interstate commerce by depressing or degrading the output and quality of apps

available nationwide, S.B. 142 necessarily has the practical and *per se* unconstitutional effect of regulating commercial and speech-related activities that occur wholly outside Utah, 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 Utah statute.

157. Unless declared invalid and enjoined, S.B. 142 will operate to unconstitutionally burden interstate commerce in violation of the Commerce Clause.

COUNT VIII
Ex Parte Young
EQUITABLE RELIEF

158. Plaintiff incorporates all prior paragraphs as though fully set forth herein.

159. S.B. 142, 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).

160. This Court can and should exercise its equitable power to enter an injunction precluding Defendants from enforcing S.B. 142 against Plaintiff's members.

COUNT IX
DECLARATORY RELIEF

161. Plaintiff incorporates all prior paragraphs as though fully set forth herein.

162. Utah Code §§ 13-76-201(1)(a)-(e), (2)(a)-(b); 13-76-202(1), (2)(a)-(b)(3), (4)(a)-(b); 13-76-402(2) violate the First Amendment of the Constitution and the Due Process Clause and thereby deprive Plaintiff, its members, and its members' users of enforceable rights.

163. 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).

164. This Court can and should exercise its equitable power to enter a declaration that the challenged provisions of S.B. 142 are unconstitutional and otherwise unlawful, both facially and as-applied.

PRAYER FOR RELIEF

Plaintiff respectfully requests an order and judgment:

- A. Declaring that Utah Code §§ 13-76-201(1)(a)-(e), (2)(a)-(b); 13-76-202(1), (2)(a)-(b), (3), (4)(a)-(b), 13-76-402(2) are unlawful;
- B. Declaring that Utah Code §§ 13-76-201(1)(a)-(e), (2)(a)-(b); 13-76-202(1), (2)(a)-(b), (3), (4)(a)-(b), 13-76-402(2) facially violate the First Amendment to the Constitution;
- C. Declaring that Utah Code §§ 13-76-201(1)(a)-(e), (2)(a)-(b); 13-76-202(1), (2)(a)-(b), (3), (4)(a)-(b), 13-76-402(2) violate the First Amendment to the Constitution as applied to CCIA’s members;
- D. Declaring that Utah Code §§ 13-76-201(1)(b)-(c), 13-76-201(2)(b), 13-76-202(1)(b)-(c), 13-76-202(3), 13-76-202(4)(b), 13-76-402(2) do not require app stores and developers to age-rate apps and in-app purchases or to use the Act’s age categories to do so;

- E. Declaring that Utah Code §§ 13-76-201(1)(b)(ii), (1)(c), (2)(b); 13-76-202(1)(b)-(c), (3); 13-76-202(4)(b); 13-76-402(2) are void for vagueness, both facially and as-applied;
- F. Declaring that the entire Act is preempted by the Commerce Clause;
- G. Enjoining Defendants and their agents, employees, and all persons acting under their direction or control from taking any action to enforce the challenged portions of S.B. 142 against Plaintiff's members;
- H. Enjoining Defendants and their agents, employees, and all persons acting under their direction or control from promulgating rules pursuant to § 13-76-301;
- I. Entering judgment in favor of Plaintiff;
- J. Awarding Plaintiff 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
- K. Awarding Plaintiff all other such relief as the Court deems just and proper.

Dated: February 5, 2026

Respectfully submitted,

/s/ Deno Himonas

Deno Himonas (5483)
Brian Willen (*pro hac vice*)
Lauren Gallo White (*pro hac vice*)
Elizabeth Sharkey (18655)
Edward Percaprio (*pro hac vice*)
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

*Attorneys for Plaintiff Computer &
Communications Industry Association*