

# Age-Gating for Contract, not Content

BRAD LITTLEJOHN

---

## The Policy Question

Child online safety is now a bipartisan policy concern at the federal and state levels, but the legal strategies employed to achieve it have produced inconsistent results. Strategies focused on restricting children from accessing age-inappropriate content, such as pornography, have received recent Supreme Court validation. But attempts to broaden this principle to other forms of content, or to social media generally, face both constitutional and political headwinds. The ungoverned online exposure children face is downstream of a more fundamental flaw in the digital economy: Digital markets engage children directly as customers, bypassing their parents. Today, most online experiences are mediated by apps or platform-based accounts, which require users to agree to “Terms of Service,” a contract governing the collection of data and the provision of services, even when no money is exchanged.

*Should policymakers subject online contracts to age verification and require parental consent for minors to access digital services?*

---

## Why It Matters

America’s children face a host of perils when they go online, which they increasingly must do to engage in their social and educational lives—communicating with friends, doing their homework, or even participating in youth sports. From the moment a child gets a smartphone (which the average child now does at age 11<sup>1</sup>), she is subjected to powerful and even addictive algorithms that lead to excessive screen time, anxiety, and sleep deprivation.<sup>2</sup> Games are designed to engage users for as long as possible, and then induce them to pay for more features. On many popular platforms, like Instagram or TikTok, the algorithms can encourage social comparison that causes depression and body dysmorphia, often leading to eating disorders, self-harm, and suicide, made worse when platforms present videos recommending such behavior.<sup>3</sup> In the private messaging features of such platforms, they risk encountering sexual predators posing as fellow teenagers, who pressure children to share nude photos, pursue sextortion

---

1 *Cell Phone Statistics 2026*, ConsumerAffairs (updated Jan. 2026).

2 For the fullest summary of harms, see Office of the U.S. Surgeon General, *Social Media and Youth Mental Health: The U.S. Surgeon General’s Advisory* (May 23, 2023). More concisely, see The White House, *The MAHA Report: Make Our Children Healthy Again*, pp. 53–55 (May 2025).

3 *The Facebook Files*, Wall Street Journal (Sept. 2021); Tawnell D. Hobbs, Rob Barry & Yoree Koh, *‘The Corpse Bride Diet’: How TikTok Inundates Teens With Eating-Disorder Videos*, Wall Street Journal (Dec. 17, 2021); for one particularly egregious example that resulted in the death by self-asphyxiation of a ten-year-old girl, see *Anderson v. TikTok, Inc.*, 116 F.4th 180 (3d Cir. 2024).



blackmail schemes, and, in some cases, use location-sharing data to prey on children in person.<sup>4</sup> Most recently, with the proliferation of AI platforms, children have been subjected to cascades of deepfake pornography, sexually explicit “AI companions,” and chatbot suicide coaches.<sup>5</sup>

Nearly all of the platforms responsible for these harms collect and monetize children’s private data, which is then used to refine the algorithms to exploit children’s weak points.<sup>6</sup> Instagram has estimated that the lifetime value of each teen user is \$270, a figure that predates the creation of chatbots to elicit children’s most private thoughts.<sup>7</sup> As the digital economy becomes more ubiquitous and algorithms more powerful, policy has not kept pace with these realities.

---

## State of Play

A bipartisan child online safety movement has mobilized against these and other harms, securing political and legal victories. School phone bans have proliferated, and age verification, once considered technologically infeasible and constitutionally dubious, has become an emerging industry standard in domains such as pornography, online gambling, and alcohol and cannabis e-commerce. The tech industry’s broad shield from liability for the content it delivers—codified under Section 230 of the *Communications Decency Act of 1996*—has begun to crack under a barrage of lawsuits.<sup>8</sup> Nonetheless, arguments against protecting kids, rooted in certain interpretations of the First Amendment, parental rights, and fear of overregulation, continue to hold sway.

Initially, parents’ groups mobilized around legislative approaches that regulate the product design of platforms likely to be accessed by minors. The *Kids Online Safety Act* (KOSA), first introduced by Sens. Richard Blumenthal (D-CT) and Marsha Blackburn (R-TN) in 2022, would impose a “duty of care” on such platforms, requiring them to “exercise reasonable care in the creation and implementation of any design feature to prevent and mitigate” harms to minors, including sexual exploitation, addictive use, self-harm, and more.<sup>9</sup> It passed the Senate 91–3 in July 2024, only to die in the House of Representatives. Despite broad political support and efforts in Congress to revive it, the legislation’s fate remains uncertain. Although proponents sought to frame the proposal as a regulation of design features rather than content outputs, opponents continue to argue it could be used to censor expression. A similar (though less carefully written) state-level law, the California Age-Appropriate Design Code,

---

4 See Nat’l Ctr. for Missing & Exploited Children, *CyberTipline Data*. See also Thorn & National Center for Missing & Exploited Children, *Trends in Financial Sextortion: An Investigation of Sextortion Reports in NCMEC CyberTipline Data* (June 2024). For a recent example of a sexual predator using app location-sharing data to carry out rape, see [Andy Brownell, Rochester Man Admits Raping Girl He Contacted Through Snapchat](#), KROC News.

5 Kashmir Hill, *A Teen Was Suicidal. ChatGPT Was the Friend He Confided In.*, N.Y. Times (Aug. 26, 2025); Thorn, *Deepfake Nudes & Young People: Navigating a New Frontier in Technology-Facilitated Nonconsensual Sexual Abuse and Exploitation* (Mar. 2025).

6 For instance, in congressional testimony, Sarah Wynn-Williams, former Director of Global Public Policy at Facebook, stated that Facebook tracked when teen girls deleted selfies so that it could target them with ads for beauty products. [Transcript: Former Exec Sarah Wynn-Williams Testifies on Facebook's Courtship of China](#), TechPolicy.Press (Apr. 10, 2025).

7 Maura Barrett, *Jury Finds Meta and YouTube Liable in Landmark Social Media Addiction Trial*, WXYZ Detroit (Mar. 25, 2026).

8 For a good summary of the emerging cracks in Section 230 immunity, see Dynamis LLP, *Section 230 Under Fire: Recent Cases, Legal Workarounds, and Reforms*.

9 Kids Online Safety and Privacy Act, [S. 2073](#), 118th Cong. (2024).



has been mired in First Amendment litigation.<sup>10</sup>

Age-verification laws, by contrast, have gained considerable traction over the past three years, and have fallen into three general approaches, achieving different levels of legal success.

The first and most successful models focused on pornography, that is, content obscene with respect to minors. Louisiana's HB 142, the trailblazer on this front, was passed almost unanimously in summer 2022 and took effect January 1, 2023, requiring any websites whose content consisted of at least 33% "material harmful to minors" to implement robust age verification to limit access to adults only. Over the next three years, two dozen states enacted similar laws. Texas's version of the law, HB 1181, was upheld by the Supreme Court by a 6–3 ruling in *Free Speech Coalition v. Paxton* (2025), reversing *Asbcraft v. ACLU*'s 2004 precedent against age verification for pornographic websites.<sup>11</sup> The court's application of intermediate scrutiny suggests that "age verification may survive constitutional scrutiny when it enforces restrictions the state has the authority to impose."<sup>12</sup>

In the case of obscene content, this authority is uncontested. But it remains disputed in other domains. Laws applying age verification to social media have been slower to gain traction, given that "social media" is difficult to define and much social media content is both unobjectionable and clearly constitutionally protected. Only nine states have passed laws outright restricting social media accounts for those under a certain age (usually 16), and nearly all those laws have been quickly enjoined, although some injunctions have been stayed on appeal.<sup>13</sup> Technically, these laws regulate the creation of user accounts and so could reasonably be construed as regulating a business relationship rather than content. However, since only "social media" platforms were required to verify a user's age, courts have tended to construe these as attempts to restrict access to specific forms of constitutionally-protected online content, triggering strict scrutiny and preliminary or permanent injunctions.

The newest approach to regulation has focused on age-gating at the mobile app store level, recognizing an app's terms of service as a contract. The leading model, the *App Store Accountability Act*, introduced at the federal level in May 2025 by Sen. Mike Lee (S. 1586), has three key elements. First, it requires Apple's App Store and Google Play to maintain age category data on users, and, if the user is under 18, to link them to a supervising parental account. Second, it requires that posted age ratings for all apps contain clear guidance for parents on the content and experiences offered by the app. Third, it requires parental consent each individual time a minor wishes to download a new app or make in-app purchases.<sup>14</sup> Passed last year in Utah, Texas, and Louisiana, the law is also gaining traction in Congress. Texas's ASAA, SB2420, was preliminarily enjoined by a district judge in January 2026, though is likely to prevail on a pending appeal to the Fifth Circuit.<sup>15</sup> Meanwhile, Google and Apple have begun

---

10 *NetChoice, LLC v. Bonta*, No. 25-2366 (9th Cir. Mar. 12, 2026).

11 See *Free Speech Coal., Inc. v. Paxton*, No. 23-1122 (U.S.). For a summary of the case and its significance, see Brad Littlejohn, *The Internet Comes of Age*, Commonplace.

12 Meg Leta Jones, *How a Texas App Store Case Could Reshape Child Safety Laws*, Nat'l L. Rev.

13 Most significantly, last year the Supreme Court refused an emergency application to block enforcement of Mississippi's social media law. *Supreme Court Allows Mississippi Restrictions on Children's Social Media Access to Remain in Place*, SCOTUSblog (Aug. 2025).

14 See Digital Childhood Alliance, *App Store Accountability Act*.

15 *Computer & Commc'ns Indus. Ass'n v. Paxton*, No. 1:25-CV-1660-RP (W.D. Tex.).



supporting the *Parents over Platforms Act* (POPA), which is structurally similar but replaces the ASAA's mandatory mechanisms with essentially voluntary compliance.

These legislative efforts have coincided with ongoing debate over the *Children's Online Privacy Protection Act of 1998*, commonly known as COPPA. The law prohibits companies from collecting personal data on users under the age of 13, a provision most platforms comply with simply by requiring anyone opening a user account to enter a date of birth from more than 13 years ago. Not only is this “actual knowledge” standard ineffective as an age-gate, but the law has been increasingly construed as making 13 the age of “internet adulthood,” such that teens were treated as fully competent digital market participants. Indeed, until early this year, Google would send children an email on their thirteenth birthday inviting them to take full control of their accounts and suspend any unwanted parental controls.<sup>16</sup> Legislative proposals for a “COPPA 2.0,” the *Children and Teens' Online Privacy Protection Act*, were introduced in both the House and Senate last year to partially address these issues: H.R. 6291, sponsored by Reps. Tim Walberg (R-MI) and Laurel Lee (R-FL), and S. 836, sponsored by Sen. Edward Markey (D-MA) and Sen. Bill Cassidy (R-LA).

---

## Analysis

Contract-based approaches have a great deal to recommend them, both conceptually and constitutionally, as a complement to other approaches. Right now, the digital economy treats minors as direct market participants, capable of entering into legally binding contractual agreements. This is historically anomalous and runs counter to the norms that prevail outside of the digital economy. As legal scholar Meg Leta Jones writes,

“Minors’ contracts have long been voidable under the infancy doctrine, which is why businesses routinely require parental consent for significant commercial relationships like opening a bank account. States have explicitly required parental consent for certain transactions and relationships including employment and medical services. Apple’s own terms of service state: ‘These terms and conditions create a contract between you and Apple.’”<sup>17</sup>

From a constitutional perspective, this contract-based approach may avoid many of the thorny questions that have dogged other attempts to legislate for child online safety. When the issue is framed as protecting minors from dangerous content, such laws invite strict scrutiny unless the content falls into clearly unprotected categories of speech like obscenity (and even this category was far from clear until 2025’s *Free Speech Coalition v. Paxton* decision.) While First Amendment rights are weaker when it comes to minors,<sup>18</sup> and courts may well rule in favor of content-based age gates as well, regulations of conduct are comparatively straightforward. As attorney Joel Thayer has written in the *Harvard*

---

16 Rebecca Ruiz, [Google Family Link Parental Controls Turn Off at 13](#), Mashable (Jan. 2025).

17 Jones, *supra* note 12.

18 As Clarence Thomas wrote in an influential dissent, “The practices and beliefs of the founding generation establish that ‘the freedom of speech,’ as originally understood, does not include a right to speak to minors (or a right of minors to access speech) without going through the minors’ parents or guardians.” *Brown v. Entm’t Merchs. Ass’n*, 564 U.S. 786, 839 (2011) (Thomas, J., dissenting).



*Journal of Law & Public Policy*, “The [app store] regulation is legally indistinguishable from any other commercial regulation...because, in commercial transactions, the sellers and distributors are generally required to know whether they are engaging with a minor or at the very least know the identity with whom they are contracting.”<sup>19</sup>

Apple and Google have already conceded this principle when it comes to in-app purchases, after a 2014 FTC consent decree,<sup>20</sup> but seek to maintain that app access itself is not a commercial transaction. However, this ignores the fact that in the digital economy, data is the most valuable currency, which is why so many apps choose to offer their services for “free.” In reality, these terms of service still represent an exchange of great value to app developers. Given the common law principle that a contract exists where the parties have exchanged something of value, there is every reason to treat app terms of service as contracts—ones that minors are not competent to consent to.

From a technological perspective, this approach is attractive. Privacy advocates have long complained that age-verification measures would threaten online anonymity and require all users to upload highly sensitive personal data to untrustworthy platforms. In fact, numerous privacy-preserving third-party age verification techniques now exist, including zero-knowledge proofs that involve no transmission of personally identifying information to a platform.<sup>21</sup> And in any case, Apple’s App Store and Google Play already maintain age data on users and family accounts in order to comply with the 2014 FTC consent decree when it comes to in-app purchases, using indicators such as credit card, email address, and user behavior; the *App Store Accountability Act* simply demands that they extend this infrastructure to share age signals with all apps at the time of download. Moreover, many platforms already target ads to users based on age data they can reliably guess from user behavior; it is disingenuous for platforms tailoring beauty product ads to 13-year-old girls to claim they have no idea which users are minors. Only in rare cases do app stores require any additional means of age verification, and once verified, the age signal can be transmitted to any application, with no need for re-verifying for individual platforms.

Moreover, although it might at first seem that protections at the app-store level would leave minors highly exposed to web-based interactions that circumvent apps, in fact the large majority of web traffic now flows through mobile devices, 94% of which is app-based rather than browser-based.<sup>22</sup> These numbers are even higher for children and teens, for whom iPads (at younger ages) and smartphones (at older ages) are the default form of internet access. Indeed, popular teen platforms such as Instagram and TikTok receive more than 90% of their traffic from mobile devices.<sup>23</sup> Thus, while not a panacea, app store-level age verification would be a meaningful policy lever for re-empowering parents to mediate their children’s access to the online world while stricter age-related bans work their way through the

---

19 Joel Thayer, *The Case for App Stores to Age Gate Harmful Online Products*, 16 Harv. J.L. & Pub. Pol’y Per Curiam (Summer 2025).

20 FTC, In the Matter of Apple Inc., Consent Agreement (Jan. 15, 2014).

21 The Age Verification Providers’ Association website currently lists no less than fifteen common methods; for fuller argumentation of how minimal the data collection and sharing needs to be for modern digital age verification, see Brief of the Manhattan Institute as Amicus Curiae, *Free Speech Coal., Inc. v. Paxton*, No. 23-1122 (U.S. Nov. 22, 2024).

22 *Digital 2025: Device Trends for 2025*, DataReportal (2025). Moreover, browser-based access is much less of an issue from a child protection standpoint, since Apple and Google phones both ship with robust parental control features for their native browsers, Safari and Chrome respectively.

23 *Mobile Website Traffic Statistics and User Data 2026*, Quantumrun (2026).



political process and the courts.

These considerations lay behind the crafting of the *App Store Accountability Act*. However, when Judge Robert Pitman of the Western District Court of Texas enjoined the law (Texas SB2420), his decision made almost no reference to the Act's core premise of regulating commercial conduct, rather than content. Based on narrow exemptions for apps that do not require user accounts or which give access to public services (exemptions the federal version of the Act wisely avoids), the judge characterized the law as a “content-based” regulation of speech, and then charged that it unreasonably restricted speech which could not plausibly be harmful to minors.<sup>24</sup>

Advocates argue that the law was never meant to protect minors from specific categories of harmful speech, but to protect them from entering into any commercial relationships without parental consent, regardless of the benevolence of the merchant or safety of the content. Given the District Court's questionable construal of the statute, and the recent precedent of *Paxton* (which similarly began with a Texas District Court injunction before Supreme Court vindication), it seems likely that the *App Store Accountability Act* will be upheld as the legal process unfolds.

These broader considerations should also be applied to the debate over COPPA reform. As of April 2026, negotiation was ongoing between the House and Senate, and within the House, on the precise terms of COPPA 2.0—particularly regarding how to define a more robust knowledge standard, and whether teens, or only their parents, can consent to data collection. However, both House and Senate proposals continue to frame the issue of data collection as one of privacy violation, rather than commercial exploitation. Legislators must recognize that since data is the currency of the digital domain, minors should not be employed as data miners for the largest companies on earth when they are too young to consent to such contracts.

---

## Recommendations

Policymakers should reject the default assumption that, so long as parents, companies, and policymakers provide protection from a handful of online “red light districts,” children should have the same unrestricted access to the internet that adults do. Businesses should not, as a matter of course, be able to mine children's data, hook them on addictive products and services, and secure their contractual consent to opaque “terms of service” that turn them into a lucrative commodity for advertisers. Policymakers should establish a new default expectation, based in longstanding principles regarding the regulation of contracts, that children's access to the digital marketplace must be mediated by parents, who must be effectively present as a “co-signer” any time a child wants to create a new account or enter into an app-based service agreement.

Two immediate steps federal policymakers can take:

- Congress should pass the *App Store Accountability Act* in its current form. The ASAA places the primary burden of compliance where it belongs: at the Apple and Google app

---

<sup>24</sup> *Computer & Commc'ns Indus. Ass'n v. Paxton*, *supra* note 15, at 9–15.



stores which serve as intermediaries of the entire mobile marketplace. It does not solve for every online harm, and, absent other measures, it leaves a burden on parents to contend against social pressure for their children to have “must-have apps” like Instagram and TikTok. But it would establish a critical new baseline, bringing the digital world into better conformity with the legal norms that govern the analog world.

- Congress should reject the *Parents Over Platforms Act* (POPA) which Apple and Google have supported as an alternative to ASAA. While superficially similar, it replaces almost all the mandatory requirements of the ASAA with voluntary self-regulation (including treating a child’s own self-reported age as their verified age). If tech companies want the opportunity to self-police their conduct, they need to demonstrate an affirmative interest in doing so, rather than playing fast and loose until the regulatory response is imminent.
- COPPA should be comprehensively reformed so that the age of “internet adulthood” is raised to 18, minimally guaranteed by a strong constructive knowledge standard, if not age verification, and with mandatory parental consent. Moreover, legislators should take the opportunity to reframe COPPA not on the narrow grounds of data privacy but on the broader grounds of contractual incapacity. Coverage should extend to any platform deriving commercial value from minor users’ data or behavior, crucially including artificial intelligence systems that are now using children’s data for training. In such a form, COPPA would be an effective complement to the *App Store Accountability Act*, requiring the development of similar mechanisms of parental notification and consent at the platform level to those which ASAA applies at the app store level. Together, they would ensure that whether using mobile apps or browsers, children would enter into digital contracts only through parental authorization.