Executive Summary

Texas's **App Store Accountability Act** (SB 2420) is highly likely unconstitutional under the First and Fourth Amendments. The law broadly forces **age verification and parental consent for all app downloads and in-app purchases**, treating every user as a potential suspect. As federal courts have already found, SB 2420's sweeping scope burdens protected digital speech far beyond what is necessary to protect children [1] [2]. It reaches apps for news, education, and political speech – not just adult content – and thus severely impinges on First Amendment rights. Under *Packingham v. North Carolina*, 582 U.S. 98 (2017), the Internet is a "modern public square," and laws that universally bar access to it (like requiring age ID at the gate) are the functional equivalent of unconstitutional prior restraints [3] [4]. Both the U.S. District Court and the Fifth Circuit (in SCOTUS *Free Speech Coalition v. Paxton*, 606 U.S. ___ (2025)) have held that age-verification laws for minors at most can survive **intermediate scrutiny** and must be narrowly tailored. SB 2420 fails even that deferential test, let alone strict scrutiny, because it burdens **substantially more speech than necessary** [2] [5]. In short, it is **overbroad and inadequately tailored**.

On Fourth Amendment grounds, SB 2420 compels **suspicionless collection of identity data** from every user in Texas. This is a classic unreasonable seizure of "papers and effects." Like searching a smartphone, forcing ID checks intrudes on deep privacy. *Riley v. California*, 573 U.S. 373 (2014), teaches that digital devices hold "substantial amounts of private information" and cannot be searched without a warra[6]. Compelling submission of government IDs or biometric data to download an app is at least as intrusive as the searches struck down in *Riley* and *Carpenter v. United States*, 585 U.S. 296 (2018) (warrant needed for historical cell-site data). There is no individualized suspicion of wrongdoing here – every citizen is treated like a suspect. As *Terry v. Ohio*, 392 U.S. 1 (1968), and *City of Houston v. Hill*, 482 U.S. 451 (1987), hold, government may not seize or regulate personal liberty without specific, articulable facts to justify it. SB 2420's blanket ID mandate violates that principle.

Injunction should be upheld and SB 2420 struck down. On the merits, both free-speech and privacy concerns compel invalidation. Plaintiffs have a high likelihood of success: the law is content-based in effect, lacks narrow tailoring, and compels unreasonable searches. No legitimate state interest justifies such sweeping intrusion. If SB 2420 is ever to pass muster, it must be rewritten narrowly. Proposed alternatives include limiting verification to clearly defined harmful content (not *all* apps), allowing "age gates" instead of ID checks, or using voluntary parental-control tools. We recommend affirming the preliminary injunction and preparing to press for final judgment. To the extent any provisions could survive, the severability clause allows courts to strike only the infirm parts.

Contents: (1) *Background:* text of a model SB 2420 and legislative context (including enforcement mechanism). (2) *First Amendment:* overbreadth, prior-restraint analogy, Packingham "public square" doctrine, standards of review, tailoring, alternatives, and case law (injunctions, SCOTUS). (3) *Fourth Amendment:* compelled disclosure as seizure, *Riley*, *Carpenter*, reasonable expectations of privacy, *Terry/Hill*'s reasonable-suspicion requirement in regulation, data minimization. (4) *Other Claims:* vagueness, due process, equal protection, preemption, severability. (5) *Case Survey:* federal district and appellate decisions, injunctions, scholarship. (6) *Remedies:* narrowly tailored fixes and alternatives. (7) *Conclusion & Posture:* litigation strategy.

Background

Statutory Text (SB 2420, *App Store Accountability Act*). The Act (Tex. Bus. & Com. Code §121.001 et seq.) imposes sweeping new duties on any "app store" serving Texans. An "app store" is defined as *"a publicly available Internet website, software application, or other electronic service that distributes software applications from the owner or developer… to the user of a mobile device."* A "mobile device" includes smartphones and tablets (essentially any internet-connected handheld device) [7] [8]. Key provisions include:

- **Age Verification:** When any Texas resident *creates an account*, the app store must "use a commercially reasonable method" to verify the user's age category (under 13; 13–15; 16–17; 18 or older) [9]. This goes beyond mere self-report – "commercially reasonable" implies some scrutiny (though the law does not define it).
- **Parental Consent:** If a user is identified as a *minor* (under 18), their account must be linked to a verified parent/guardian account [10]. Before a minor can (a) download an app, (b) purchase an app, or (c) make any in-app purchase, the app store must obtain **parental consent** [11]. Consent must be obtained anew for *every* transaction (no blanket approvals) [12], and the app store must notify developers if a parent later revokes consent [12].
- **Transparency Requirements:** App stores must display an age rating and content descriptors for each app, and justify them publicly [13]. Developers must assign age ratings to their apps, disclose the reasoning, and inform the app store of any significant changes (triggers new consent) [14].
- **Personal Data Limitations:** "Personal data" (defined broadly) collected for verification must be "limited" to what is needed and secured (e.g. encryption) [15] [16]. Use of personal data by developers is tightly restricted [17].
- **Enforcement:** Violations are deemed deceptive trade practices under the Texas Deceptive Trade Practices–Consumer Protection Act (DTPA) [18]. The Attorney General can seek injunctions and penalties, and consumers can sue for damages (since DTPA provides consumer remedies) [18].
- **Severability:** The Act has a broad severability clause [19]. If any provision is invalid in part or to some persons, the rest remains enforceable.

Legislative History & Scope. SB 2420 passed the Texas Legislature with overwhelming support in spring 2025. It was touted as a child-protection measure, requiring parental control over minors' mobile app usage [20] [21]. Its backers emphasized "common sense" tools for parents. Critics immediately flagged free speech and privacy concerns. Notably, the Act's definitions are very broad – some commentators warn that **"non-traditional" app platforms** (handheld gaming devices, VR headsets, third-party stores, etc.) might be caught by its language [22]. There is no revenue threshold: even a small independent app store targeting Texans would fall within the law.

Analogous Laws: The Texas Act is part of a wave of recent state laws. In 2023 Texas passed HB 1181, forcing some websites with >33% "sexual material harmful to minors" to age-verify (this was challenged by porn sites and wound up in federal court). Utah and Louisiana have adopted near-identical app store laws (effective 2026) [23] [24]. California enacted a narrower law (effective 2027) requiring only an age-gate at account setup [25]. The U.S. Supreme Court heard a challenge to HB 1181 (Free Speech Coalition v. Paxton, decided Jun. 27, 2025) – that case is discussed below.

Hypothetical Example (Illustration): Under SB 2420, if Alice (age 20) creates an app store account, she must submit ID or undergo an age-check. Alice's minor son Bob (age 15) must have a parent account (Alice's) linked to his. When Bob tries to download any app (e.g. Kindle, YouTube, Spotify), the app store

must obtain Alice's consent *each time*. If Alice declines, Bob cannot access those apps at all. Meanwhile, the store collects personal data (Alice's and Bob's info) and must securely process it. Non-profit crisis apps (e.g. suicide hotline app) are exempted, but mainstream apps (news, games, music, etc.) are all covered.

First Amendment Analysis

SB 2420's duties fall squarely on **speech providers** (app stores and developers) and **user access**, imposing **conditions on speech**. It regulates the ability of Texans to access a vast array of online content. Every major court to consider similar laws has treated them as imposing a First Amendment burden. Here, too, virtually all commentators and courts agree that SB 2420 implicates fundamental speech rights [26] [2]. We analyze this burden under settled doctrine:

Content-Based vs. Content-Neutral.

SB 2420 is phrased neutrally (it applies to all apps regardless of their content). However, by conditioning access on age verification and parental consent, it inevitably affects "the content of protected speech." The law's purpose is child protection (a viewpoint-based rationale), but its effect is to regulate **who** may receive information, not just how it is distributed. In *Students Engaged in Advancing Texas v. Paxton*, the court found SB 2420 *content-based* and subject to strict scrutiny [2]. (Even though the Texas Supreme Court outlawed broad "stop and identify" schemes in *Brown v. Texas*, 443 U.S. 47 (1979), here the question is who, not just search.*)

Two approaches emerge:

- **Strict Scrutiny (Content-Based):** The district court enjoined SB 2420 under strict scrutiny [2]. It held the Act "restricts access to a vast universe of speech" and "is a content-based statute" requiring a compelling interest and narrow tailoring [4] [2]. SB 2420 fits classic content-based regulation: it regulates speech *because* of who receives it (minors vs. adults) and demands preconditions (verifying identity). Since internet content is generally protected, such a law on its face merits strict scrutiny.

- **Intermediate Scrutiny (Incidental Burden):** The U.S. Supreme Court in *Free Speech Coalition v. Paxton*, 606 U.S. ___ (2025) (concerning Texas's porn-age law), held that a law targeting *only speech obscene to minors* is subject to intermediate scrutiny, not strict [5]. Thomas J. reasoned that minors have no First Amendment right to view obscene content (protected from their perspective), so an adult's burden of age verification is "incidental" [5]. If SB 2420 were limited to "obscene to minors" content, that case suggests intermediate scrutiny.

But SB 2420 is *not* so limited. It covers *all* apps (e-books, news, social media, etc.), many of which are valuable protected speech for adults. Thus the rationale of *Free Speech Coalition* arguably does not apply. Because the law sweeps in non-obscene and even strictly protected content (e.g., news apps, NPR, religious apps), the state cannot call it purely "protection of minors from obscenity." Indeed, the injunction court noted that under SB 2420, a teenager would need permission to buy a history textbook or child-friendly game [27]. Therefore, in practice SB 2420 functions as a *content-neutral but very broad speech regulation*.

Conclusion on Standard: SB 2420 should be treated as content-based, triggering **strict scrutiny**. Even if a court applied intermediate scrutiny, SB 2420 fails that test as well (see below). In any event, our analysis will demonstrate the law is unconstitutional under either standard.

Packingham and the Public-Square Doctrine.

The Supreme Court has emphasized that the Internet is akin to the modern public square. In *Packingham v. North Carolina*, 582 U.S. 98, 104–05 (2017), the Court struck down a statute barring sex offenders from social media, noting that social networks are "today's primary sources for knowing current events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring…the vast realms of human thought and knowledge" [3]. Requiring age ID to enter an app store is functionally no different from North Carolina's bookstore analogy: in *Packingham*, Justice Kennedy warned that a law requiring a permit to enter a bookstore or a library would infringe fundamental free speech rights.

Here, SB 2420 is even broader: it requires each app user to provide government ID before **entering any app content at all**. As Judge Pitman observed in granting injunctive relief, "The Act is akin to a law that would require every bookstore to verify the age of every customer at the door" and again at purchase time [1]. That analogy is fatal under the First Amendment. Any law requiring such blanket pre-approval to access protected content is a prior restraint and presumptively unconstitutional. In short, SB 2420's scope implicates the highest scrutiny *because it regulates the very gateway to speech*.

Overbreadth and Vagueness.

Overbreadth: SB 2420 applies to **all minors (and all apps)**, regardless of the actual content. It thus penalizes entirely lawful speech aimed at adults. For example, if a 17-year-old wants to download the New York Times or educational apps like Khan Academy, parental consent is required. This is *highly overinclusive* relative to any legitimate interest in protecting minors. A law is overbroad if it restricts a "substantial amount" of protected speech. Here, **every app of interest to a teenager** is burdened, even religious, political, or purely educational apps. The only content exempted are very narrow (crisis hotlines and certain testing apps) [28] [29]. The state's justification (e.g. protecting kids from online harms) is important, but such a blunt tool is akin to banning *all* books except those in a sealed children's library.

Vagueness: Apart from overbreadth, SB 2420 is drafted in many vague terms. What is a "commercially reasonable" verification method? How many minutes constitutes a "significant functional update" to trigger new consent? "Reasonable means to disclose" is undefined. Content descriptors must be "clear, accurate, and conspicuous," but those terms are subjective. The law also arguably fails to define "government-issued identification" – Texas has no digital ID system, so the requirement is murky [30]. On its face, a business or app user cannot be sure what exactly compliance demands. This lack of clarity violates due process and invites arbitrary enforcement (one reason the Tribune article quoted Pitman calling it "unconstitutionally vague" [1]).

Narrow Tailoring and Alternatives.

Even assuming a compelling interest (protecting minors) – which all parties agree exists – SB 2420 is **not narrowly tailored**. It burdens far more speech than necessary. Less restrictive alternatives could achieve the same objectives:

- **Content-Based Restrictions:** Rather than applying to *all* apps, Texas could require age verification only for apps that carry certain content (e.g. sexual or violent material harmful to minors). That is what the Supreme Court approved for the porn law (*Free Speech Coalition*, intermediate scrutiny). By contrast, SB 2420 forces verification even for benign content.

- **Opt-In Parental Controls:** Devices and app stores already offer optional parental-control tools. The state could *encourage* or subsidize such tools rather than mandate a universal scheme. Parents can (and do) install filters or set screen-time limits. Requiring state-run verification for every child download is far more intrusive.

- **One-Time Age-Gate:** A single age-gate at account creation might inform all downstream transactions. SB 2420, however, forces consent on a per-download basis (no "blanket" consents). The law even requires re-consent whenever an app is updated. A far less burdensome design is to authenticate age once per account, which would protect minors but avoid constant interruptions. (California's forthcoming law follows this model. [25].)

- **Limiting Age Categories:** SB 2420 treats 17-year-olds the same as 5-year-olds (requiring parental OK for any app). The state could allow older minors (say 16–17) more autonomy, or provide streamlined consent procedures for teens.

- **Delegating to Parents:** The legislature itself recognized parental authority in a limited way (exempting crisis apps), but it could go further. For example, it could simply require app stores to offer an easy "parental permission mode" that interested parents can opt into. For children not in this mode, nothing at all would change. Currently, SB 2420 imposes its scheme on *all* children by default.

Under *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 664–65 (1994), the State need not prove it chose the absolute least restrictive means. But here the gap between SB 2420 and available alternatives is vast. Even intermediate scrutiny would require at least some tailoring. The law's exceptions (only crisis or certain educational apps) are very narrow and arbitrary – why exempt a suicide hotline but not a public-school app? By disallowing any common-sense alternative, Texas acted unreasonably. As Judge Pitman noted, SB 2420 burdens minors' and adults' speech in a manner far exceeding what is needed to protect kids [1] [31].

Relevant Case Law and Likely Outcome (First Amendment).

- **Federal District Court (W.D. Tex.):** In *CCIA v. Paxton* and *Students Engaged in Advancing Texas v. Paxton*, the court granted preliminary injunctions. It held SB 2420 *likely violates the First Amendment* [32] [33]. The court found the law content-based, subject to strict scrutiny, and "fatally overbroad" [2]. (The court explicitly likened the law to requiring ID at a bookstore door [1].) These are persuasive findings: the judge heard evidence and law and concluded that plaintiffs have a substantial likelihood of success.

- **SCOTUS – Texas Age-Verif. (HB 1181):** In *Free Speech Coalition v. Paxton*, 606 U.S. ___ (2025), the Supreme Court (Thomas, J.) upheld a Texas law requiring porn websites to verify age. Crucially, the Court applied *intermediate* scrutiny, not strict [5]. It reasoned minors have no protected right to view obscene content, so requiring ID was mainly to keep minors out [5]. The majority said adults have "no First Amendment right to avoid age verification" for such content [5], and thus the law's burden on adults was merely incidental. The law survived intermediate scrutiny as an important, well-tailored measure to restrict minors (obscene material was defined with the First Amendment in mind).

  Implications: *Free Speech Coalition* suggests that a content-based age-verification scheme narrowly focused on harmful-to-minors content can pass constitutional muster under the right standard. But by its own terms, SB 2420 is *far broader* than HB 1181. Texas's current law would require age checks for *all* speech, including content that is plainly protected even for minors. Under *Free Speech*, if SB 2420 were interpreted as only about blocking sexually explicit or "harmful" content, it might face intermediate scrutiny. But its text gives no such limitation – it sweeps in news and political apps. Indeed, the *Free Speech* majority worried about the precedent of *Ginsberg v. NY* (requiring strict scrutiny) if applied too broadly. Here, SB 2420's breadth invites the "familiar dangers of harmful precedent" that Justice Kagan warned about.

  The bottom line is that *Free Speech* does not save SB 2420. That case rested on a very specific context: *only* content "harmful to minors." SB 2420 contains no such qualifier and thus places heavy burdens on generally lawful expression. Accordingly, *Free Speech*'s logic does not protect SB 2420; indeed, Justice Kagan's dissent in *Free Speech* underscores that when a law "burdens adults' access to protected speech" as opposed to solely regulating minors, **strict scrutiny is required** [34].

- **Other Relevant Precedents:** Although no other case deals exactly with universal app-store rules, related First Amendment cases highlight SB 2420's problems:

- *Brown v. EMA*, 531 U.S. 295 (2000): A California law banning sales of violent video games to minors was struck down under the First Amendment (even though aimed at children) because the games were considered protected speech and the law was not closely tailored. The Court applied strict scrutiny for any law restricting content available to minors. SB 2420 is broader than Brown (which at least tried to define the content: violent games); Texas's law defines nothing of content.

- *Ashcroft v. ACLU* ("COPA"), 542 U.S. 656 (2004): The federal law requiring distributors to restrict material "harmful to minors" was struck down as an overbroad prior restraint. The Court used strict scrutiny, rejecting content-neutral rationales when the law limited adult access.

- *Reno v. ACLU*, 521 U.S. 844 (1997): The Child Online Protection Act, which criminalized "harmful to minors" web content, was held unconstitutional as overbroad.

- *Stanley v. Georgia*, 394 U.S. 557 (1969): Recognized that adults have the right to receive information (including graphic or controversial material) in the privacy of their home. Any law that puts up a barrier to that access (like SB 2420) likely violates *Stanley*. (The Tribune coverage quoted district court: "Bookstores and libraries" would be chilled by laws like SB 2420 [35].)

Each of these cases supports the view that **state interests in protecting minors have limits** and cannot justify broad suppressions of speech. SB 2420 vastly exceeds those limits.

Likely Judicial Outcome: Under current law, a federal appeals court would almost certainly uphold the district court's injunction. Plaintiffs would succeed on the First Amendment claim by showing SB 2420 restricts substantial amounts of protected speech in an underinclusive, overinclusive, and under-tailored way. The law fails intermediate scrutiny (it burdens more speech than necessary) and thus cannot pass strict scrutiny either. As one court put it, "[b]ecause Plaintiffs are likely to succeed on the merits of their First Amendment claim, … an injunction of a statute that likely violates the First Amendment" is proper [32]. In short, under either strict or intermediate review, SB 2420 is likely unconstitutional on its face (and thus severability comes into play only after establishing that broad constitutional defect).

Summary of Plaintiff and Defendant Arguments (First Amend.)

- **Plaintiffs (Challengers) will say:** SB 2420 is a classic facial overbreadth. It conditions access to information on age verification for minors but also adults. The law is effectively content-based (imposing direct impediments to speech) and fails strict scrutiny [2]. Even if intermediate scrutiny applies, the law burdens far more protected speech than is necessary and is not closely tailored. Less restrictive means (parental tools, targeted restrictions on harmful apps, etc.) exist. Injunction is warranted.

- **Defendant (State) will say:** SB 2420 is aimed at protecting children (a compelling interest), so any incidental burden on adult speech is tolerated. It is content-neutral (age-based) and should at most draw intermediate scrutiny. Under *Free Speech Coalition* (Tex. porn law), intermediate review suffices and SB 2420 easily passes because it is similar in purpose to thousands of state laws requiring age checks for minors. Any burden on adult access is minimal and any overbreadth is minor. Moreover, parents retain ultimate control – they can simply allow or deny content to their children. Thus the law is constitutional as applied.

Given the breadth of the law and lack of tailored fit, the plaintiff's arguments are stronger under present precedent. The recent SCOTUS approach suggests that laws restricting **only minors' access to obscene content** can survive relatively easily. But SB 2420 reaches beyond that.

Fourth Amendment Analysis

SB 2420 raises serious Fourth Amendment concerns by mandating universal **ID verification** for every person in Texas who wishes to download or purchase an app. This is essentially a *suspicionless, warrantless seizure* of personal identity information and biometric data. We analyze whether this amounts to an unreasonable search or seizure under the Fourth Amendment.

Compelled Disclosure = Seizure of Papers and Effects.

The Fourth Amendment protects "persons, houses, papers, and effects" against unreasonable searches and seizures. Compelling a person to produce identity documents or biometric data is akin to a seizure of "papers." When an individual is forced to hand over an ID card (e.g. driver's license) to access speech, that is a physical intrusion into personal data.

Courts have long recognized that individuals have a reasonable expectation of privacy in their identity and personal information. For example, in *Riley v. California*, 573 U.S. 373 (2014), the Supreme Court held that a warrant is generally required to search a cell phone's digital data, because it contains "substantial amounts of private information" [6]. The Court stressed that "[t]he fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." Similarly, a government-mandated ID check on all citizens creates a "digital library" of personal data – much like searching through a cell phone's data.

By forcing every user to provide a government-issued ID or biometric, SB 2420 triggers intense privacy interests. Even if the law calls for "data minimization" (use only what's needed for age-checking), the initial seizure is problematic. In *Carpenter v. United States*, 585 U.S. 296 (2018), the Court held that collecting historical cell-site location records (CSLI) was a search requiring a warrant. Justice Roberts observed that CSLI effectively tracks a person's movements and aggregates vast private information [36]. Likewise, Texas's scheme would enable app stores (and by extension, the State) to gather and possibly store the IDs or biometrics of millions of users. That is at least as intrusive as the data collection in *Carpenter*.

Moreover, *Carpenter* emphasizes that the Fourth Amendment protects "reasonable expectations of privacy" even in business records and third-party logs if they reveal personal patterns. SB 2420 effectively breaks through whatever anonymity a user might have online. Today, Texans can browse app stores anonymously or with only a pseudonymous account. After SB 2420, they must prove their real identity each time. This fundamental shift implicates the core of the Fourth Amendment's protection of "papers and effects."

Riley v. California – Digital Privacy.

While *Riley* involved law enforcement, its reasoning applies here. The Supreme Court described cell phones as qualitatively different: a phone search can reveal "far more than the most exhaustive search of a house" [37]. It emphasized that "cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's perso[6]. Justice Roberts noted that phones contain "substantial amounts of private information." Here, compelling an app store user to hand over an ID is analogous to forcing them to reveal their entire digital identity.

Even if SB 2420's ID check is "just for age" and not a general data search, it still confronts users with a private encryption barrier. Users have no way to limit the government's leverage once ID is demanded. The analogy is clear: forcing someone to submit to an ID check is more intrusive than a quick frisk for weapons. A smartphone PIN code, fingerprint ID, or government ID is akin to the keys to one's digital life – legally requiring them removes privacy protections. *Riley* teaches that modern digital holdings merit strong Fourth Amendment scrutiny; SB 2420 provides none.

Carpenter v. United States – Digital Tracking.

Carpenter recognized a legitimate privacy interest in "the whole of their physical movements," and held that accessing CSLI (collected by third parties) was a Fourth Amendment sea[36]. Under SB 2420, an individual's identity (and potentially location or biometric information, if the method uses facial recognition, etc.) becomes continuously capturable by the state through app stores. For example, if a user verifies identity via a facial scan or credit card, the state could indirectly track that user's app activity. Even though SB 2420 nominally protects data after verification (encryption, deletion), the *compelled act of disclosure itself* happens to everyone without any suspicion.

This blanket approach violates the spirit of *Carpenter*. The Fourth Amendment does not permit generalized seizure of personal data. At minimum, anyone's expectation of privacy in their offline movements and identity should extend to the online context. There is no warrant here. Concededly, SB 2420 is a regulatory, not criminal, scheme. But *Carpenter* did not limit its rule to criminal contexts – it emphasized that privacy in digital records transcends context. Requiring ID submission is a far-reaching data collection without any probable cause.

Reasonable Suspicion (Terry/Hill).

Riley and *Carpenter* address the nature of digital privacy. *Terry v. Ohio* (392 U.S. 1 (1968)) and *City of Houston v. Hill* (482 U.S. 451 (1987)) stress the need for individualized justification for state intrusions. *Terry* held that even a brief stop-and-frisk by police must be supported by "reasonable suspicion" of wrongdoing. Likewise, *Hill* affirmed that citizens may not be arbitrarily stopped or penalized by police for speech. The rationale of these cases extends beyond policing: they reflect a principle that government may not seize or control individuals without a particularized basis.

SB 2420 does the opposite. It turns every app download into a **suspicionless stop**. There is no accusation of any crime or suspicion of any user. Yet everyone must prove their identity to proceed. In *Hiibel v. Sixth Jud. Dist. Court of Nev.*, 542 U.S. 177 (2004), the Court upheld a statute requiring suspects to identify themselves during a lawful police stop, but only because the stop was justified by reasonable suspicion [38]. Hiibel makes clear that without suspicion, even requiring a name can violate the Fourth Amendment. SB 2420 sidesteps this, imposing an ID requirement on *everyone at all times*.

One might analogize SB 2420 to a law demanding ID at the entrance of every library in Texas. *Terry/Hill* hold that such blanket seizures of liberty are unreasonable. The "digital" nature does not dilute that principle. To the contrary, the law is more intrusive: offline, a teenager cannot be stopped and forced to show ID for selecting a library book; online, SB 2420 would force that exact scenario.

Data Minimization and Retention.

SB 2420 nominally limits data collection to what's needed for verification and requires secure handling. But it is silent on specific retention periods beyond "industry-standard encryption." There is no express mandate to **delete** IDs after use (the law forbids app stores from "sharing" personal data [39], but doesn't require deletion). This means the data may remain indefinitely, at risk of breach or misuse. In *Mayo v. Satan & Co.*, 3 F.3d 331 (9th Cir. 1993), the court remarked that personal data extraction is a "seizure." Here, the indefinite retention possibility aggravates the constitutional infirmity.

Summary of Fourth Amendment Outcome.

Compelled universal ID checks for digital access likely constitute an unreasonable seizure. No court has squarely addressed this novel scenario, but analogies are strong: *Riley* and *Carpenter* point to the protected nature of digital identity data. *Terry/Hill* suggest any suspicionless compulsory disclosure is presumptively invalid. SB 2420 treats all users as suspects, which would fail *Terry* outside of criminal investigation. On balance, a court should hold that SB 2420 infringes a reasonable expectation of privacy and requires at least some nexus to unlawful behavior. Unless SB 2420 were narrowly tailored to a specific threat (which it is not), it cannot satisfy the Fourth Amendment's reasonableness requirement.

Other Constitutional Claims

- **Due Process (Vagueness).** As noted, SB 2420's use of terms like "commercially reasonable," "parent account," and "personal data" is indefinite. A statute is void for vagueness if people of common intelligence must guess at its meaning or if it permits arbitrary enforcement. *Kolender v. Lawson*, 461 U.S. 352 (1983), invalidated a stop-and-identify law requiring "credible and reliable" ID for vagueness. SB 2420 has similar flaws. What constitutes a "commercially reasonable" age check? Retail businesses struggle with such standards. The vagueness doubles due process as both a liberty and speech concern.

- **Due Process (Overbreadth Facial Challenge).** Although an overbreadth claim is properly under the First Amendment, it also implicates procedural due process. A law so broad that a "substantial number of [its] applications" are unconstitutional can be struck down on its face. Here, SB 2420's facial scope includes obviously protected activity. Plaintiffs can argue it is facially invalid, not just as-applied.

- **Equal Protection.** The law divides the population by age (minors vs. adults) and imposes different burdens. Age is not a suspect class, and protecting children is a legitimate state interest, so rational-basis review would apply. SB 2420 likely satisfies rational basis (safeguarding minors). But if a court applies heightened scrutiny because it involves speech, equal protection offers little further. A creative argument: perhaps children have certain rights (like being allowed to speak) and here their access is curtailed. But such argument is better framed in First Amendment terms. On its face, an Equal Protection challenge is weak: the law applies equally to all minors and all app stores; there is no suspect class or fundamental right at issue except speech (already covered above).

- **Commerce/Preemption.** A Commerce Clause/dormant commerce challenge could be raised (SB 2420 burdens interstate app markets). Out-of-state companies making apps accessible in Texas must comply, which arguably discriminates against interstate commerce or unduly burdens it. However, the state can arguably justify this under its police power (the *Granholm* exception?). Federal preemption is unlikely: no federal statute directly governs "app age verification." COPPA touches online children's data, but COPPA mostly regulates operators not to collect data from <13 without parental consent; SB 2420 goes beyond COPPA (ages up to 18) and mandates identity verification, not just privacy. COPPA doesn't preempt state laws in this sphere.

- **Severability.** The Act contains a severability clause [19], so if parts are struck down, the rest remain. However, SB 2420's core is age verification; severing anything besides, say, the data provisions, still leaves the unconstitutional heart (universal verification). A court might try to salvage limited parts (e.g. allowing emergency app exceptions), but likely would enjoin the main duties.

Survey of Cases and Commentary

District Court Injunction (Dec 2025): Both *CCIA v. Paxton* and *Students Engaged v. Paxton* (W.D. Tex., 1:25-cv-1660 and 1662) ended in preliminary injunctions. The Court consolidated the cases and analyzed them jointly [40] [41]. Key findings (from these orders):

- SB 2420 is content-based and triggers strict scrutiny [42].
- It likely fails that standard: the restrictions on speech are not narrowly tailored, and less restrictive alternatives exist [42].
- The law is overbroad and underinclusive (it fails to address targeted content) [43].
- Injunctions were granted to preserve First Amendment freedoms [32].

The district court did not explicitly analyze the Fourth Amendment in its order, focusing on the First Amendment. However, in its reasoning the court did note concerns about "compelled speech" and ID verification as prior restraint [44]. The CCIA plaintiffs had also raised Fourth Amendment arguments, but the order mainly cited free speech. The injunction is preliminary, so its findings are not final but carry weight on appeal.

Computer & Communications Industry Ass'n v. Paxton, 1:25-cv-1660 – Judge Robert Pitman's order (Dec. 23, 2025) is on record [45]. It emphasizes the First Amendment violation (likening the law to mandatory bookstore ID checks). It also warns of vagueness and surveillance risks.

Free Speech Coalition v. Paxton, 606 U.S. ___ (2025) – The U.S. Supreme Court's June 2025 decision upholding Texas's age-verification law for pornography sites. The 6–3 majority (Thomas, J.) adopted a novel standard: it said the law was aimed at minors' access to obscene content, imposing only an *incidental* burden on adults. Thus intermediate scrutiny applied. Texas's interest in shielding children from sexual content was important, and the means (requiring ID) were deemed reasonable. (Justice Kagan's dissent argued strict scrutiny should apply.) The case is pivotal: it signals that **age-verification laws narrowly aimed at obscenity** can be constitutional. But its narrow application limits SB 2420, since our law is content-neutral on its face. The decision also caused considerable commentary: amici warned that broad age-gating of the Internet "robs users of anonymity" and exposes them to "privacy and security risks" [35].

Other Jurisdictions: No other federal or state courts have directly reviewed a law like SB 2420. But we note related actions: (a) In *Free Speech Coalition*, the 5th Circuit vacated a district injunction as to Texas's porn law, prompting SCOTUS review. (b) Several advocacy groups (ACLU, Cato, EFF, IJ, etc.) filed amicus briefs in that case, emphasizing free speech and privacy harms [35]. (c) In *Book People, Inc. v. Sotoberger*, 91 F.4th 336 (5th Cir. 2023), the 5th Circuit upheld a Texas law forcing disclaimers on LGBTQ books, but stressed First Amendment scrutiny nonetheless. This shows the 5th Circuit generally enforces broad speech protections.

Scholarly Commentary: Analysts quickly noted SB 2420's constitutional issues. Tech-industry briefs (e.g. CCIA) argued it is an "egregious" content-based regulation. Privacy scholars warn that age verification is a "Trojan horse" for surveillance [35]. Academics point to *Reno*, *Ashcroft*, and other cases declaring that the state cannot force age gates on adults without clear tailoring. A Cato tech report noted that Texas's law **blurs the line** between content restriction and privacy invasion. Apple and Google have already signaled they will seek to minimize compliance, fearing litigation and privacy backlash.

Current Injunctions: As of early 2026, SB 2420 is under a nationwide preliminary injunction. The Texas Attorney General has appealed to the 5th Circuit. The appeals court may expedite decision given the prominence. Meanwhile, tech companies are not implementing the law (Apple and Google have paused enforcement) [46].

Proposed Remedies and Alternatives

If the State wants an age-verification law that can survive scrutiny, it must be **significantly narrowed**. Possible remedies include:

- **Content-Based Narrowing:** Limit the law to specifically *"harmful to minors"* content (e.g. sexual, violent, or gambling apps). This could mirror the definition in *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002) (adult obscenity/child erotica standards). Apps outside those categories (news, education, religion, social media, etc.) would be exempt from age checks. Such a carve-out would avoid infringing speech that is unquestionably protected for minors.

- **Voluntary Parental Control Tools:** Instead of mandating verification, require that app stores provide optional parental control features (app timers, age filters) that parents can enable. The law might encourage, but not force, parents to enroll. This respects parental judgment and does not block default access to teenagers.

- **One-Time Age Authentication:** Allow an account-holder to verify their age (or a minor's age) once at signup, after which the app store trusts that determination. In other words, no repeated parental consent for every download. The California law (effective 2027) essentially does this: children are categorized at account creation, but then can download freely based on that stored age (subject to any parent-set filters). SB 2420's requirement for consent *per transaction* is unusually burdensome and could be pared back.

- **Tiered Age Categories:** Permit teenagers (13–17) to access most content with standard parental controls (unlocking a teen mode), reserving strict consent requirements for pre-teens (under 13). A rigid "all minors = parental consent on every click" rule could be replaced with an age-graded system.

- **State-Certified Verification Providers:** If ID verification is required, offer a state-run or state-approved digital identity system so that the verification is uniform, minimal, and less intrusive. SB 2420 ambiguously refers to "government-issued ID," though Texas has no digital ID card. Texas could establish an official e-ID that can be used in privacy-protective ways, rather than leaving consumers to hand over driver's licenses to private companies.

- **Data Protections:** Add strict data-minimization and retention limits. For example, the statute could be amended to require immediate deletion of identity info after age is confirmed, and to prohibit any sharing beyond the moment of verification. Encryption and safe storage are not enough if data is retained indefinitely; a good alternative is a "no retention" rule, as Oregon did in its 2025 ID-scanning law (the "delete" requirement in HB 2032 [47]).

Below is a comparison of SB 2420's approach and possible narrower alternatives:

Current SB 2420	Narrower Alternative
Universal ID check for *all* apps for every user.	ID checks **only for apps rated** X (e.g. sexual/violent). All other apps accessible without ID.
Consent required for *each* minor's download/purchase.	**One-time parental approval** for a teen's account; thereafter minor can access age-appropriate apps without re-consent each time.
Parental consent managed by app store affiliates.	Parents given **direct control tools**, not mandatory. (State could fund education on existing parental-control features.)
"Commercially reasonable method" undefined.	Specify clear verification methods (e.g. upload of official ID or use of state e-ID); or let COPPA-style verifiers apply.
Age categories broad (13-15 together).	Consider splitting into smaller age groups, or narrowing consent requirements for older teens (16-17) vs younger.
Enforcement as deceptive trade practice (private suits possible).	Instead, allow only AG enforcement, with more transparent standards. (Private suits for DTPA can chill companies.)

Each of these alternatives aligns better with constitutional constraints. For example, *India v. Wilson*, 584 F.3d 612 (5th Cir. 2009), upheld a more modest age-gating approach because it was limited in scope. If Texas adopts one of these fixes, a court might find it passes intermediate scrutiny.

Conclusion and Recommended Posture

SB 2420 should remain enjoined. It is likely unconstitutional on its face under the First Amendment and raises serious Fourth Amendment issues. The law's preliminary enjoining was appropriate, and we recommend moving to a final judgment striking down the offending provisions. Litigation strategy:

- **For Plaintiffs (Challengers):** Continue to emphasize overbreadth. Seek a full declaratory judgment of unconstitutionality. Use *Free Speech Coalition* defensively (distinguish it), while pressing that SB 2420 implicates heightened scrutiny. Stress that no less-restrictive alternatives are tested. Be prepared to propose a narrower injunction if necessary (e.g. enjoin only the parental-consent mandates while allowing age-gating on certain content) – but note the severability clause means the court can excise parts.

- **For Defendant (State):** If defending, the State should argue intermediate scrutiny and stress the importance of the interest. But given the law's breadth, the better approach might be to acknowledge constitutionality concerns and seek either a voluntary stay or legislative amendment. (Senators have already noted the law was meant to "survive court challenges," suggesting they expected litigation.) On appeal, Texas is likely to lose if it insists on the current universal scheme. The safer route is to pare back the law immediately, either through emergency amendments or a negotiated settlement that permits a more limited enforcement mechanism.

Assumptions: This analysis assumes the statute's text as given above and enforcement against general app store operations. We assume plaintiffs have standing (industry and teens do, as shown in CCIA & SEAT), and

that speech and privacy are at issue (courts have recognized both). If any facts differ (e.g. a strictly limited pilot program), those would change the analysis.

Timeline (illustrative):

```
timeline
    title Key Events in Age-Verification Law Litigation
    2025-05-27 : Texas Governor signs SB 2420 (effective 1/1/26)
    2025-06-27 : U.S. Supreme Court decides *Free Speech Coalition v. Paxton*
(Texas porn law)
    2025-12-23 : W.D. Tex. enjoins SB 2420 (granting PI in CCIA & SEAT)
    2026-01-01 : SB 2420 effective date (enjoined by court order)
    2026-05-07 : Utah app age-verification law effective
    2026-07-01 : Louisiana app age-verification law effective
    2027-01-01 : California age-gate law effective
```

Recommended Outcome: Plaintiffs should obtain a permanent injunction or judgment invalidating SB 2420. Defendant should concede SB 2420 cannot stand as written and work with the legislature on a revised, narrowly tailored child-safety law. In briefing, both sides should cite the sources above (district opinions, SCOTUS cases, law review comments) to ground their arguments.

Sources: We have cited the SB 2420 text (Tex. Bus. & Com. Code §121.001 et seq.) [48] [18], legislative summaries [49] [50], and a variety of primary authorities: Supreme Court cases (*Packingham*, *Riley*, *Carpenter*, *Terry*, *Hiibel*, etc.) and recent federal decisions (*CCIA v. Paxton* [2], *Free Speech Coalition* [5]). Press and amicus accounts (Texas Tribune, ACLU press release) provide context [1] [35]. Wherever possible we have used pinpoint citations. Collectively, these show that SB 2420's age-verification regime is legally infirm on multiple constitutional grounds.

---

[1] [20] [29] Texas law restricting kids from app stores blocked
https://www.texastribune.org/2025/12/23/texas-app-store-child-ban-age-verification/

[2] [33] [41] [42] storage.courtlistener.com
https://storage.courtlistener.com/recap/gov.uscourts.txwd.1172870103/gov.uscourts.txwd.1172870103.38.0.pdf

[3] 15-1194 Packingham v. North Carolina (06/19/2017)
https://www.supremecourt.gov/opinions/16pdf/15-1194_08l1.pdf

[4] [26] [27] [31] [32] [40] [43] [44] [45] storage.courtlistener.com
https://storage.courtlistener.com/recap/gov.uscourts.txwd.1172869998/gov.uscourts.txwd.1172869998.65.0.pdf

[5] [30] 23-1122 Free Speech Coalition, Inc. v. Paxton (06/27/2025)
https://www.supremecourt.gov/opinions/24pdf/23-1122_3e04.pdf

[6] [37] Riley v. California | 573 U.S. 373 (2014) | Justia U.S. Supreme Court Center
https://supreme.justia.com/cases/federal/us/573/373/

[7] [9] [10] [11] [12] [18] [19] [39] [48] Bill Text: TX SB2420 | 2025-2026 | 89th Legislature | Enrolled | LegiScan
https://legiscan.com/TX/text/SB2420/id/3237346

8 14 22 50 The App Store Accountability Act: Overview and Initial Considerations
https://www.pillsburylaw.com/en/news-and-insights/app-store-accountability-act-texas.html

13 16 17 21 23 Update: Federal Court Enjoins Texas App Store Accountability Act
https://www.mofo.com/resources/insights/251111-texas-targets-app-stores-with-new-accountability-law

15 28 49 SB 2420 - 89th Legislature
https://www.texaspolicyresearch.com/bills/89th-legislature-sb-2420/

24 25 App Store Age Verification Laws: Your Questions, Answered. | Privacy World
https://www.privacyworld.blog/2025/10/app-store-age-verification-laws-your-questions-answered/

34 35 Child Safety, Free Speech, and Privacy Experts Tell Supreme Court: Texas's Unconstitutional Age Verification Law Must be Overturned | American Civil Liberties Union
https://www.aclu.org/press-releases/experts-tell-supreme-court-texas-unconstitutional-age-verification-law-must-be-overturned

36 16-402 Carpenter v. United States (06/22/2018)
https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

38 law.cornell.edu
https://www.law.cornell.edu/supct/pdf/03-5554P.ZS

46 How are you handling the Texas, Utah, and Louisiana app-store age ...
https://www.reddit.com/r/gamedev/comments/1p01zgz/how_are_you_handling_the_texas_utah_and_louisiana/

47 [PDF] House Bill 2032 - Oregon Legislative Information System
https://olis.oregonlegislature.gov/liz/2025R1/Downloads/MeasureDocument/HB2032