



Bill Study

App Store Accountability Act

August 2026

How to read this report

This bill study is organized into nine sections as follows:

- The [Executive Summary](#) provides a synopsis of the bill study and presents the key takeaways;
- [Key Concepts](#) provides definitions for important terms used throughout the report;
- The [Introduction](#) explains what is the problem addressed in the bill, what evidence supports the problem, and why it matters to the Commonwealth;
- [Understanding Age Assurance](#) provides a technical overview of the methods for assessing the age of users and the tradeoffs in accuracy, privacy and accessibility;
- The [Policy Landscape](#) compares Virginia's introduced bill to legislation in other states and reports what is known about their outcomes;
- Finally the [Policy Recommendation](#) section puts forth several recommendations for policymakers to consider.

The report can be read as a continuous document, or be skipped to sections of interest. The main compelling ideas are presented in the Policy Recommendation section.

Executive Summary

This study reviews the evidence surrounding age assurance and considers the concerns raised by placing age verification and parental consent duties at the app store level. Available data supports the concerns that prompted SB237, but it does not show how often these harms occur or how effectively app store age verification would prevent them. Furthermore, similar laws in other states have been enacted within a short time frame and have yet to produce measurable results. In addition, recent age assurance legislation in other states has been subject to litigation, substantial amendments, and delays in implementation.

The study presents five recommendations for policymakers to consider. First, to improve the quality and reliability of information users have about apps, an independent body should audit age ratings and content descriptions assigned by app developers. Second, to decrease the risk of consent fatigue, parental controls should be easy to understand and use, and controls should be set to the highest default safeguards with options to remove safeguards. Third, to improve the information policy makers and technologists have about risks and harms, users should have a clear way to report adverse experiences in app stores. Fourth, parental consent should apply only to apps whose age rating exceeds

the user's age category, or to apps that involve purchases. Finally, to enhance accountability, app store providers should collect and publicly report the data needed to assess how these requirements work in practice.

Key Concepts

Age assurance: Refers to the overarching methods employed to establish, verify or estimate the age or age range of an individual. These methods include age verification, age estimation, and age inference; a fourth approach, age attestation, involves no confirmation and is treated as a weak control. Furthermore, these methods provide different degrees of certainty and may have different implications for privacy, costs, accuracy, and accessibility [1, 2]. Age assurance does not necessarily require confirmation of identity: age can be treated as a separate attribute from identity

Age attestation: A declaration of age made by a user, or by another person on the user's behalf, without a direct confirmation from official identification documents. Attestation is not among the three core methods recognized in the international standard on age assurance [1], which treats an unchecked declaration as a weak control. Nonetheless, app store accountability acts in the US allow an affirmative attestation by a parent or legal guardian of a minor as a method for satisfying the requirements in age-category verification [3-6].

Age estimation: An age assurance method that analyzes biological or behavioral attributes associated with age to determine the age or age range. Facial analysis is one common example of this method. Since this estimation produces a likelihood rather than a factual confirmation, errors may occur near the legal age thresholds that determine eligibility [1, 7].

Age inference: An age assurance method that uses verified information to draw an indirect conclusion about the age or age range of an individual. Such information may include for instance, the ownership of a financial product that is available only to adults [1].

Age rating: One or more classifications that indicate the suitability of the content and functions on an app or in-app purchase, to the user associated with an age category. Under app store accountability acts, the developer is responsible for assigning the age ratings. However, unlike other types of ratings (e.g., films), app ratings are not required to be issued or validated independently.

Age signal: Information related to an age category or age range that an operating system or app store transmits to a developer. Developers may use the signal to apply age-related restrictions and protective settings. An age signal communicates information about age rather than a decision made by a parent concerning a particular app. Major technology platforms have begun providing age signal interfaces, although the access is generally limited to jurisdictions where legislation requires the service [8, 9].

Age verification: An age assurance method that calculates the age of a user from a date of birth confirmed from an official source (e.g., passport or driver's licence). Age verification offers the strongest assurance but it also excludes users who do not possess the required documents [1].

App store: An online resource that is publicly available (i.e., website, software application, or other electronic service or platform) and allows account holders to download and install apps created by third-party developers.

Content description: A description of the specific elements or functions that inform an app's age rating. In general, the developer is required to provide both the app content description and the age rating.

Data minimization: The principle that an organization should collect only personal data that is adequate and reasonably necessary for a disclosed intention. Data minimization is a core requirement of the Virginia Consumer Data Protection Act [10, 11].

Significant change: A modification to the terms of service or privacy policy of an app that changes the categories of data collected, stored, or shared. The term also includes changes to the age rating or content description, and applies when an app adds in-app purchases or advertising that it did not previously include. The term was first used in Utah's App Store Accountability Act from 2025 and was adopted into the state bills that followed. The closest analogue in federal law is the "material change" under COPPA.

Verifiable parental consent: An authorization granted by a parent or legal guardian before a specified action involving a minor may proceed. Under COPPA, the term refers to consent for the collection, use, or disclosure of personal information from a child younger than 13 [12].

Zero-knowledge proof (ZKP): A cryptographic method that allows an individual to prove a claim, such as being older than 18, without disclosing an underlying identity document or other personal information. ZKP-based age assurance has been deployed by the European Commission and by Google Wallet [13, 14].

Introduction

For the last decade, mobile applications ("apps") have been the primary way for young people to engage with the digital world, and app stores have been the most popular means of accessing those apps. An app store allows an individual to download mobile apps created by third-party developers onto a mobile device. Apple and Google are the two largest app store providers, although other companies also operate app stores. Most of the mobile apps that are used by young people today, including games, social media, text messaging services, and chatbots, can be downloaded through an app store. A 2024 Pew Research Center survey found that 95% of U.S. teenagers ages 13 to 17 had access to a smartphone at home, and nearly half said they were online almost constantly [15]. The US Surgeon General

similarly reported that approximately 95% of adolescents use at least one social media platform, with more than one-third using social media almost all the time [16].

There has been an increase in public concern regarding the amount of time children spend using digital media and the specific content they engage with. The Centers for Disease Control and Prevention (CDC) in its 2023 Youth Risk Behaviour Survey found that 16% of US high school students experienced cyberbullying during the previous year [17]. Additionally, the Surgeon General reported that approximately two-thirds of adolescents across the US were often or sometimes exposed to hate-based content on social media [16]. A separate study by Common Sense Media found that 73% of teenagers between 13 and 17 had seen pornography on the internet. It is noteworthy that among all respondents, 29% reported having encountered that content only by accident, without ever intentionally searching for it [18]. A separate report by the same organization found that nearly three in four teenagers had used AI companion applications, with half using them regularly, and that around one-third of those users had felt uncomfortable with something an AI companion said or did [19]. The Federal Trade Commission has since opened an inquiry into how providers of such applications evaluate their safety for children and teenagers, although that study is not an enforcement action and has not yet been reported [20]. App stores do not directly cause these harms because harmful conduct occurs after accessing an app. However, app stores constitute an important gatekeeper in accessing the content consumers are concerned about. Therefore, app stores may be an important site for intervention before a minor engages with harmful content.

App store users have historically had limited information available before deciding whether to download an app. In a 2012 review of children's mobile apps, the Federal Trade Commission found that disclosures about data collection and in-app purchases were often missing before installation. Only 20% of the apps provided a privacy disclosure before download, and only 15% disclosed advertising, even though 58% contained it [21]. In addition, the FTC found that the information provided after download could be too late for parents or guardians to take action, as children may have already been using the app or a parent may have already been charged [22]. Although these findings are over ten years old, more recent research suggests that the gap has not been closed. A 2023 study of 20,195 Google Play apps for children found that approximately 81% of those designed exclusively for children used trackers, and that around 19% reported age ratings that were inconsistent across rating authorities [23]. Additionally, a 2026 study of nearly six thousand child-accessible mobile apps found that while both major app stores (i.e., Apple and Google) provide privacy labels for mobile apps, there was a high level of inconsistency between the labels an app displayed on each store, indicating that these disclosures do not reliably reflect what an app actually collects and shares [24].

One of the most clearly documented concerns is financial harm. For example, in 2014, as part of a settlement agreement with the FTC, Apple agreed to issue at least \$32.5 million in refunds to parents who were charged for purchases made by their children without their consent [25]. As of June 2025, the FTC distributed more than \$126 million to Fortnite players as a result of complaints involving unauthorized purchases of in-game items made using the credit cards of parents without their knowledge [26].

App Store Accountability in the News

- ["Supreme Court won't block Texas app store age verification law," Reuters, 6 July 2026](#)
- ["Louisiana sues Roblox alleging the popular gaming site fails to protect children," Associated Press, 14 August 2025](#)
- ["Utah becomes first state to pass legislation requiring app stores to verify user ages and get parental consent for minors," Associated Press, 6 March 2025](#)
- ["App stores are set to verify ages under a new Utah law — and Meta, Snap, and X are thrilled," Business Insider, 6 March 2025](#)
- ["FTC Sends \\$126 Million in Refunds to Fortnite Players Who Were Charged for Unwanted Items, Reopens Claims Process," Federal Trade Commission, 25 June 2025](#)
- ["France Joins a Global Move Toward Restricting Social Media for Children," The New York Times, 21 July 2026](#)

The growing public concern on these issues has begun to translate into state law, as existing federal protections have proven inadequate for addressing the policy issues around apps. The Children's Online Privacy Protection Act (COPPA) was designed to regulate the collection of personal data for children under 13, and therefore leaves younger and older minors outside its protection [12]. Furthermore, the parental consent required by COPPA covers only the management of personal information and not the action of downloading or making app-related purchases. COPPA has many well-evidenced weaknesses in the current digital environment. The FTC released a report in 2024 detailing how major online services often treated teens no differently from adults when collecting their data, covering practices from 2019 and 2020 [27]. The report noted that most online services do not place any restrictions on minors accessing the services they offer, and it recommended that Congress extend privacy protections to minors over 13. However, Congress has not enacted such protections yet. In the absence of federal action, several states have begun to introduce their own laws to regulate the access of minors to mobile apps.

SB237 enters this developing state policy landscape with a basic premise: the tools parents need already exist, but providers do not offer them consistently, and there are no mechanisms to hold providers accountable. For example, Apple, Google, Samsung, and Amazon each already offer some capabilities for capturing age signals or requesting parental consent. However, each company makes these tools available only in the jurisdictions where legislation requires them, rather than across all markets [8, 9, 28, 29]. In some cases, providers have publicly opposed the legislation requiring these tools. For example, Google has raised concerns with age verification laws from the Texas App Store Accountability Act (SB2420)[5] in their developer manuals [30]. Similarly, Apple highlighted that those laws would require the collection of sensitive, personally identifiable information to download any app, “even if a user simply wants to check the weather or sports scores” [31].

Additionally, some evidence suggests that parents want more choices about how and when children download apps, but they also find managing children’s device use to be challenging. In a survey conducted by Pew in late 2023, it was reported that 76% of parents considered managing their children’s phone time an important or top priority, while only 47% reported that they already limit it. Additionally, 43% of parents described the task as hard, compared to 26% who found it easy [32]. In short, proposed legislation, including SB237, aims to address the challenges parents and minors are encountering when trying to exercise choice over what content they want to access. It would require app stores to provide, before every download or purchase, information that users need to determine whether to download a specific app and options for parental oversight that parents desire but currently lack in most jurisdictions.

The available evidence supports the existence of the problem that app-store age-verification aims to solve, but it does not demonstrate whether it would successfully address those concerns. Therefore, three questions remain open: 1) whether better disclosure and a parental consent requirement actually lead parents to make better decisions; 2) whether the app store is the right point of intervention, given what it can and cannot reach; and 3) whether the age of every account holder can be assessed without creating the privacy risks that the bill seeks to prevent. The sections that follow address each of these questions.

Understanding Age Assurance

In order to safeguard minors online, providers rely on a family of methods collectively referred to as age assurance, which differ substantially in how they work and what their tradeoffs are in terms of privacy, user burden, and cost. Different methods of age assurance may determine how well a legislative requirement works in practices. The international standard on age assurance (i.e., ISO/IEC 27566-1) recognizes three main methods of age assurance: verification, estimation, and inference [1].

Age verification checks a user's age against an authoritative source (e.g., passport, driver's licence, credit card, etc.). Because it relies on a verified record rather than an estimate, it provides the strongest assurance of the three methods. That higher level of certainty comes with a greater burden. Users must have and submit an official document, which may exclude people who do not possess one, and the provider must collect identity information that some users may be reluctant to share [1]. **Age estimation** does not rely on an official document. Instead, it uses physical or behavioral attributes, most commonly facial analysis, to estimate a person's age or age range. This approach may be less intrusive, but it cannot provide the same degree of certainty, particularly near legal thresholds such as the boundary between ages 16 and 18 [7]. **Age inference** uses other verified information to draw an indirect conclusion about age. For example, ownership of a financial product available only to adults may indicate that a user is over 18. The reliability of this method depends on how closely the underlying information is connected to age; a weak or indirect signal provides limited assurance.

An important concern is that age estimation, and to a greater extent age verification, may require an app store to process personal information or biometric data for every user, not only for minors. Therefore, in order to identify which users are minors, an app store provider may first assess the age for every account, effectively creating an age-gate for all users. The selected method used by an app store provider will largely determine how much data must be collected and to whom the method applies.

These methods also differ in who performs the check. An app store may assess age itself, or it may delegate the task to a specialist age verification provider. Delegation carries its own tradeoff, since it would imply sharing the user's personal information with third-parties [33]. In addition, a technical assessment published by the Knight-Georgetown Institute found that no single method is sufficient on its own because self-declaration, commercial and government records, government identification documents, and age estimation all have limitations in either precision or availability [33]. Thus, the report suggests that a good age assurance system must support several methods, so that the user can use alternatives in case one of these is not applicable in a specific situation.

Many legislative requirements to safeguard minors do not specify the technical means of age assurance, leaving this determination up to providers. This ambiguity introduces additional risks: mandating age assurance may give providers a blank slate to collect even more data about all users, or it may introduce new security risks when third party age verifiers are enlisted to conduct age assurance.

Applying age assurance in app stores

The question for policymakers is whether age assurance, when applied at the app store, would protect children from the harms they encounter through apps. Answering this question requires two

conditions to hold. First, the app store must be able to establish the age category of its account holders. Second, the apps themselves must have accurate information about their content, so that an age category can be matched to an appropriate restriction. Unfortunately, currently neither condition is fully satisfied.

Placing age assurance at the app store carries a structural advantage that allows the assessment to be performed once at a single point instead of multiple times by every developer. Thus, centralizing age assurance would reduce the burden on users and the number of parties that must hold personal data. However, because age verification is associated with an individual account, it may not always be accurate in reflecting the actual age of the user operating the device at that particular time, especially if several users share a device.

The second condition concerns whether the information presented to the account holder truly reflects the app's actual content. Each app is assigned an age rating based on a questionnaire completed by the developer, without independent confirmation. On Google Play, these responses are based on the International Age Rating Coalition (i.e., IARC) system, and although member authorities may review and override a rating, they generally do so through spot checks and user complaints rather than through pre-release inspection [34, 35]. Apple, on the other hand, assigns ratings through its own questionnaire, without a coalition of rating authorities [36]. Moreover, a five-year study of the Google Play Store found that hundreds of top apps carried content ratings that did not initially match their actual content and were corrected only later. Moreover, ratings can change without notifying the user so a child who downloaded an app under one rating may afterward be exposed to content under the revised rating [37]. Furthermore, because a higher rating would result in a smaller audience, developers face a financial incentive to provide a conservative, lower self-rating in the questionnaire.

Treating the app stores as the centralized point through which minors reach apps could be classified simultaneously as *too broad* and *too narrow*. It is *too broad* in that it applies to all apps rather than only to the categories that are the most associated with online harm (e.g., social media, messaging, or content-sharing apps), extending the same requirements to apps that carry little or no relevant risk (e.g., bookstores, learning apps). There is often a misconception that what the bill proposes would be the equivalent of requesting to show an identification for a restricted item in a physical store (e.g., alcohol), however this is not a valid analogy in this context, since a store checks identification only at the moment a restricted product is purchased, whereas app-store age verification would require every user to have their age assessed simply to enter the app store, and would then require parental consent for a minor to download any app at all [38, 39]. Therefore, the requirement would arguably reach well beyond the categories of apps that motivated the bill: the age-assessment burden falls on every user, and the consent burden falls on minors across all apps rather than only those carrying age-restricted content

[39]. The technical literature supports this distinction by identifying two separate use cases for age assurance: applying “safer defaults” for general-purpose applications versus restricting access to specific content categories [33]. Of course, without accurate, independently audited age ratings for apps, there is no way to determine with certainty which apps carry higher risks for minors.

At the same time, it’s *too narrow* because minors can often access the same content outside of app stores. Although the bill’s definition of “app” is broad enough to include a web browser itself, Virginia’s proposed bill would regulate the download of apps through an app store and likely would not apply to the websites and web-based services a minor visits through a browser once it is installed. For example, a minor could download a browser, such as Google Chrome, and navigate to Instagram using a URL and log into an Instagram account through the browser—all without downloading the Instagram app. As all modern devices ship with a web browser installed, a minor would still have the ability to access a service via an Internet browser without having access to the app store or going through the parental consent process [40].

There are also additional gaps that arise at the point of distribution for mobile apps; because the bill’s definition of “app store” refers to platforms that host apps from third-party developers, a developer that distributes only its own app from its own website falls outside both the “app store” and the “developer” definitions [40, 41], and developers using payment methods outside the purchasing system of an app store must implement their own parental consent mechanisms [29]. Additional evidence suggests that when the coverage of regulations is inconsistent, users would be inclined to use the least-regulated services. For example, after Louisiana required age verification for adult websites, search interest decreased for compliant sites and increased for non-compliant sites [42]. As such, while age assurance through the major centralized app stores would encompass many of the avenues users take to download apps, it does not address web access and first-party distribution models.

Challenges to Age Assurance

There are several important challenges and critiques of age assurance, including limits of effectiveness, risks to privacy and user rights, and the implications of layering parental consent on top of age assurance mechanisms. The Knight-Georgetown Institute has evaluated age assurance systems by considering four main criteria: (i) baseline accuracy, (ii) resistance to circumvention, (iii) availability, and (iv) privacy [33]. In so doing, they found that no one mechanism works well across all four dimensions, and that these trade-offs are inherent for all current age assurance approaches, not a result of immature technology. The two subsections that follow group the criteria into two key questions: whether age assurance is effective and what it costs in terms of privacy and user rights.

A) Effectiveness

The most comprehensive assessment of these methods to date is the Australian Age Assurance Technology Trial, an independent evaluation of 48 providers and more than 60 technologies, conducted before the introduction of minimum age requirements for social media [43-45]. The trial concluded that age assurance "can be done in Australia privately, efficiently and effectively," and that there are no substantial technological barriers preventing its deployment. However, the trial did also specify that no single solution would suit all the use cases, and therefore, no specific method can guarantee to be effective in all circumstances.

To date, Australia has produced the most compelling evidence of how such requirements perform in practice. Researchers at the University of Newcastle surveyed adolescents before and three months after the Social Media Minimum Age Act took effect in December 2025, and found that more than 85% of respondents under 16 continued to access the restricted platforms, even though two-thirds of them reported encountering an age check [46]. The form of verification they encountered the most was a self-declaration of age, although the eSafety Commissioner indicated that such a method was insufficient not long before the Act took effect [72]. Between 54% and 68% continued using the accounts they had before the regulation took place, while a smaller group used fake accounts, accessed services through other people's accounts, or relied on private browsing [46]. Surprisingly, a separate survey conducted on children that still used restricted platforms found that only 4% to 5% had used a VPN or a comparable tool, and that most had not needed a workaround at all, because the platforms had never identified their accounts in the first place [47]. The authors attributed this outcome not to the ingenuity of minors but to age checks that were not effective.

Circumvention is often assumed to be the principal obstacle to age assurance, but the available evidence gives limited support to that assumption. After the United Kingdom introduced the Online Safety Act in July 2025, several VPN providers reported sharp increases on sign-ups, in some cases of more than 1,000% [48]. Although this suggests an intention to bypass age checks, it does not establish that circumvention actually occurred. Furthermore, the evidence from Australia indicates that technical circumvention occurs in a small proportion of minors who continue to access restricted platforms. A qualitative study of fifteen Australian children aged 12 to 16 found that where circumvention did occur, the most common and lowest-effort method was simply falsifying data, by entering a false date of birth or using an account belonging to an older relative or friend, rather than by defeating the verification technology itself [49]. Therefore, the more consequential limitation appears to be the weakness of the verification method itself, which is consistent with the international standard on age assurance, as it treats an unchecked declaration of age as a weak control [1]. Additionally, the technical literature indicates that all age assurance systems remain vulnerable to circumvention to some

degree, and that a system capable of preventing every minor from reaching restricted content could not be built without also excluding a substantial number of adults [33].

Age estimation also introduces a degree of uncertainty as it provides a likelihood rather than a factual confirmation of age. Independent testing showed that the accuracy is the lowest near age limits, such as between one age threshold and another [7], which numerous age restrictions in legislation are based on. Accuracy of age detection also differs among different demographic groups; women showed higher probability of mistakes and there are also differences in accuracy depending on ethnicity and skin color [7, 50]. Beyond accuracy, facial estimation can also be defeated by simple means. Children in one Australian study described holding photographs of older faces up to the camera, presenting recordings of another person completing a scan, and altering their appearance with makeup, costumes, lighting, or facial expressions in order to pass an age check [49].

Finally, effectiveness is limited by the unit being assessed. An age check performed when an app is installed does not prevent a younger user from accessing apps that an adult downloaded and verified on a shared device, such as a family tablet [51].

B) Privacy and user rights

Whether app stores can determine the age of users through a commercially reasonable method without introducing significant new risks is not well supported by the available evidence. Both the literature and conducted interviews with stakeholders suggest several reasons.

The first reason is the conflict with Virginia's own privacy law. In order to identify which users are minors, a provider must assess the age of every user, which stands in tension with the principle of data minimization. Most age assurance methods are in conflict with this principle, because assessing the age of a user requires collecting or processing personal data that a service would otherwise have no reason to hold [51]. What is more, this runs counter to the goal of data minimization; instead of collecting less, a provider must now establish an age for every user it serves [52]. This is precisely the principle codified in the Virginia Consumer Data Protection Act, which directs controllers to limit data collection to what is adequate, relevant, and reasonably necessary [10, 11].

The second reason is the data-sharing risks. Because any developer may request the age category of its users, a developer that obtains actual knowledge that a user is under 13 may thereby incur obligations under COPPA, including restricting the user's access and deleting personal information in order to remain compliant [53]. Therefore, distributing minor-status data across a large number of developers, most of whom neither need nor want it, could therefore create both large repositories of data about minors and unanticipated compliance burdens.

The third reason is the concentration of sensitive documents. Because the penalties in the bill create pressure to avoid errors, providers may gravitate toward the most definitive method available, such as collecting identification documents issued by the government, which those companies are reluctant to store because it concentrates sensitive data and increases the negative impact of potential breaches [51]. In October 2025, Discord disclosed that an unauthorized party had accessed a third-party age assurance vendor and obtained images of government-issued identification documents belonging to approximately 70,000 accounts, which users had submitted when appealing an age determination in order to comply with requirements in the United Kingdom and several US states [54]. The documents existed only because a legal requirement compelled their collection, and the loss occurred at a vendor rather than at the platform the users had chosen. This risk is most acute where thresholds below 18 are in use and minors themselves are asked to demonstrate their age [33].

In order to address the privacy concerns associated with collecting additional personal data on users, zero-knowledge proof has been proposed as a possible technical solution. A zero-knowledge proof (ZKP) would allow a user to prove a claim (e.g., being over 18) without disclosing any official document or date of birth. The method depends on the user first holding a credential issued by a trusted authority stored in a digital wallet, an application that keeps such credentials on the user's own device rather than on a provider's servers. When a service asks whether the holder is over a given age, the wallet returns only a proof of that single fact, and the underlying document is never transmitted. The European Commission and Google Wallet have already deployed this approach [13, 14]. Their use shows that stronger assurance does not always require greater collection of personal data, although adoption is still at an early stage.

The provisions in question have to do with children's rights, and not merely with those of their parents. UNICEF has stated that age limitations may have adverse effects, since online services help many children, especially those who are isolated or marginalized, to engage in learning, connection, and self-expression. Furthermore, minors excluded from regulated platforms may turn to less regulated services, where they become harder to protect [55]. Thus, measures adopted on behalf of minors may also limit rights that belong to them, including their rights to privacy and participation.

Parental Consent

Parental consent is related to age assurance, but it is not an age assurance method. Age assurance establishes how old a user is, whereas parental consent determines whether an adult approves a particular action by a minor user. A provider may therefore assess age without involving a parent in any individual decision, as the age-signal model does. Conversely, parental consent presupposes an age assessment, since a provider must first determine that an account holder is a minor. In the app store

accountability model it operates as an additional layer placed on top of age assurance, and it raises a distinct set of considerations.

The first is how parents will react to the actual consent step itself. If app-store age verification requires parents to provide verified consent prior to each download, purchase, or significant change, it's possible that this will lead to consent fatigue. When faced with repeated requests for consent, users often approve them without reading (thus, negating any opportunity for making an appropriate and informed decision) as they are overwhelmed [56]. The European Commission has acknowledged the risk of consent fatigue and the proliferation of consent prompts as a problem that needs to be resolved [57]. Therefore, whether a mandatory prompt would produce a considered decision, or instead become a reflexive click, is an open question that the existing evidence does not resolve.

The second consideration is the underuse of existing tools that are already offered to parents. A representative 2025 study found that parents underused parental controls across every device examined. Only 47% used them on smartphones, and use was lowest among parents of children with the highest levels of screen time [58]. Another recurring challenge is usability. Parents described the tools as difficult to understand and navigate, and some relied on their children for help setting them up [58]. It remains unclear whether parents would use a mandatory consent process more consistently than the optional controls many already skip.

A final concern relates to adolescent autonomy. Proposed legislation would apply to all minors under 18, but several stakeholders interviewed by JCOTS expressed that teenagers often seek more independence and that parents may want to grant older teens more freedom than the bill's model anticipates. Research on adolescent online safety suggests that highly restrictive parental controls can undermine the trust between a parent and a teenager, and may produce outcomes contrary to those intended [59-61]. Consequently, the appropriate degree of parental involvement is likely to vary according to the minor's age. A uniform treatment of all minors would not recognize the inherent diversity among minors with different developmental needs and levels of maturity.

Policy Landscape

Virginia

The App Store Accountability Act was introduced during the 2026 Session as SB237 [62] (Chief Patron: Senator Head) and as the House companion, HB757 [63] (Chief Patron: Delegate Runion). Both bills would add a new chapter (i.e., Chapter 60, §§ 59.1-614 through 59.1-619) to the title 59.1 of

the Code of Virginia and take effect on July 1, 2027. This proposed chapter places duties to app store providers and developers as follows.

Duties of app store providers:

- Provide account holders with a clear parental consent disclosure for each mobile app, covering the age rating, content description, policies for personal data collection, protection and sharing with third parties, and mechanisms for data protection.
- Determine the age category of each individual creating an account and verify its veracity using a commercially available method; for a minor, that method may include an affirmative attestation by another individual reasonably believed to be the parent or legal guardian.
- Require a minor account to be affiliated with a parent account.
- Obtain verifiable parental consent from the parent account each time before the minor downloads or purchases an app or makes an in-app purchase.

Duties for developers:

- Assign an age rating and provide a content description for each app, including information about in-app purchases, and supply each app store provider with the information needed for the parental consent disclosure.
- Verify, through the data sharing methods offered by the app store, the age category of an account holder and, for a minor account, whether verifiable parental consent has been obtained.
- Notify the app store provider of any significant change to an app.
- Use the provided age category data to enforce their own age-related restrictions, safety features, or defaults.
- Apply the lowest age category reported where multiple sources of age data possess conflicting information.
- Refrain from enforcing a contract against a minor without verifiable parental consent, misrepresenting the parental consent disclosure, or sharing age category data with anyone.

Enforcement:

- The Attorney General may bring an action in the name of the Commonwealth seeking an injunction and civil penalties of up to \$7,500 for each violation, and may also recover the costs of the investigation (e.g., attorney fees).
- A minor who suffers harm from a violation, or the parent of such a minor, may bring a civil action against the app store provider or developer, recovering the greater of actual damages or \$1,000 per

violation, along with punitive damages where the violation was egregious, plus attorney fees, expert witness fees, and court costs.

Federal and Other States

SB237 is part of a broader and increasing trend among states to regulate the access of minors to mobile apps. Comparable bills are currently under consideration in numerous states, and a federal App Store Accountability Act (S1586/HR3149) advanced out of a House subcommittee in December 2025 [64, 65].

There are currently two age assurance models that states have enacted. The first is the app store accountability model, which SB237 follows, where duties are placed on app store providers and developers to verify age categories, associate minor accounts to parent accounts, and obtain verifiable parental consent before a minor downloads or purchases an app. Utah was the first state to enact such a law in 2025 [3], and Louisiana [4], Texas [5], and Alabama [6] followed. The second is the age-signal model, adopted by California in the Digital Age Assurance Act (AB1043) [66] and by Colorado in the Age Attestation on Computing Devices Act (SB26-051) [67], which does not require parental consent for each download. Instead, it requires the operating system provider or app store to transmit an age range signal to developers, who must then apply age-appropriate protections according to the age range received.

Each of these laws also provides a good-faith safe harbor for erroneous signals. Neither of them requires a minor account to be associated with a parent account, nor do they require parental consent before a download, purchase, or in-app purchase, or renewed consent after a significant change. As discussed in the "[Understanding Age Assurance](#)" section, the age-signal model is an alternative approach that shifts the response to the developer, who holds the most relevant information about a given app. It also avoids the per-download consent step that raises the consent-fatigue concern, though at the cost of removing the parent from the individual download decision. Neither law is yet in effect, as California's takes effect in January 2027 and Colorado's in July 2028.

In addition, two key observations can be drawn from the legislative landscape. First, no state has yet produced evidence that either model works because most of these laws are not yet in effect and none has been in operation long enough to be evaluated. Moreover, none of them, including SB237, requires the collection or reporting of data that would allow its effectiveness to be measured. Second, the app store accountability model is still being revised by the states that adopted it. Utah amended its law in 2026, partly in response to litigation, and Louisiana delayed and reenacted its law before it took

effect [68], while the constitutional challenge to the Texas law remains unresolved. These changes indicate that the model has not yet reached a stable form, and that a state enacting it today may need to amend the law before it ever becomes effective.

Table 1. State and federal legislation on minors' access to mobile apps, compared to SB237

State & Bill	Status	Similarities to SB237	Differences from SB237
<i>Federal</i> S1586 / HR3149 [64, 65]	Introduced May 2025 (pending) HR3149 advanced out of a House subcommittee in December 2025	Same four age categories. Age category verification. Minor accounts are associated with parent accounts. Request for parental consent and renewal. Real time sharing of age-related data. Safe harbor for developers.	Applies only to app stores with over 5 million US users. Different labels for age categories. Enforcement by the FTC and state attorneys general. No private right of action. Would preempt state laws.
<i>Utah</i> HB498 (amends SB 142) [3]	Enacted 2025 (amended 2026) Effective May 6, 2027	Same four age categories. Age category verification. Minor accounts are associated with parent accounts. Request for parental consent and renewal. Covers preinstalled apps.	Excludes emancipated/married minors. Enforcement now by private right of action only (SB237 also authorizes Attorney General enforcement and \$7,500 penalties). No developer age rating system. No exemption for emergency services apps.
<i>Louisiana</i> HB570 / Act481, amended by HB977 [4, 68]	Enacted 2025 (delayed and reenacted by HB977 in 2026) Effective July 1, 2027	Same four age categories. Age category verification. Minor accounts are associated with parent accounts. Request for parental consent and renewal. Duties for developers in managing age-related data.	Excludes emancipated/married minors. Attorney General enforcement with a 45 day cure period and penalties up to \$10,000 per violation. No private right of action. Developers may rely on app store signals to satisfy parental consent duties rather than obtaining consent independently. Adds a "family account applications" category.
<i>Texas</i> SB2420 [5]	Enacted 2025 Effective Jan. 1, 2026 (enjoined Dec. 2025; injunction stayed by the Fifth Circuit June 2026; Supreme Court declined to block July 2026; currently in effect)	Same four age categories. Age category verification. Minor accounts are associated with parent accounts. Request for parental consent and renewal. Preconsent disclosure of rating and data practices.	Applies only to new accounts. Excludes minors whose disabilities of minority are removed. Enforced through both a private right of action and laws for deceptive trade practices. Developers must delete data after age assurance is conducted. Does not cover preinstalled apps.
<i>Alabama</i> HB161/Act 2026-59 [6]	Enacted 2026 Effective Jan 1, 2027 (Oct 1, 2027 for existing accounts)	Same four age categories. Verification for new and existing accounts. Minor accounts are associated with parent accounts. Request for parental consent and renewal. Real time sharing of age-related data.	Excludes emancipated/married minors. Enforcement only by the Attorney General as a deceptive trade action. No private right of action. The Attorney General must adopt verification rules.

		Covers preinstalled apps. Developers shall use the lowest age category received. App store safe harbor for verification on good-faith	
Florida SB1722 [69]	Rejected (not enacted)	Same four age categories. Applies to app stores, developers, and preinstalled apps. Verification for new and existing accounts. Request for parental consent and renewal. Private right of action. Enforcement through deceptive trade.	Excludes emancipated/married minors. Would require the Department of Legal Affairs to adopt verification rules. Does not expressly require developers to assign age ratings.
California AB1043 [66] (age-signal model)	Enacted 2025 Effective Jan 1, 2027	Age information shared with developers. Developers must use age information for compliance. Limits sharing age-related data with third-parties. Attorney General enforcement and civil penalties.	Regulates operating system providers and app stores. Requires an age-signal rather than parental consent. No associated parent accounts or parental consent duties. Developer deemed to have "actual knowledge" but no prescribed response.
Colorado SB26-051 [67] (age-signal model)	Enacted 2026 Effective July 1, 2028	Age information shared with developers. Developers must request and use an age-signal. Data restricted to the minimum necessary. Attorney General enforcement. Safe harbor for good faith.	Regulates operating system providers, app stores, and apps. Requires an age range-signal rather than parental consent. No associated parent accounts or consent duties. \$2,500 to \$7,500 penalty per affected minor. Exempts open-source software, business apps, and code repositories.

*Florida's SB1722 is included as a rejected bill and the federal S1586/HR3149 as a pending bill. California and Colorado follow the age signal model. All other bills follow the same app store accountability model that SB237 uses.

A note on constitutionality

In 2025, the United States Supreme Court in *Free Speech Coalition v. Paxton* [70] upheld a Texas age-verification law applying to pornographic websites. However, the basis for the Court's decision was its determination that the content at issue was obscene to minors and therefore held no constitutional protection for them. SB237 is different because it conditions access to lawful and constitutionally protected content on age assessment, rather than restricting content that is already unprotected. This distinction has already surfaced in court. In December 2025, a federal district court preliminarily enjoined Texas's App Store Accountability Act (SB 2420), finding it likely violated the First Amendment because conditioning the download of every app on age verification and parental consent was not narrowly tailored, since most apps contain speech that minors have a constitutional right to access [39]. The judge compared the law to requiring a bookstore to check the age of every customer at the door [39]. The Fifth Circuit stayed that injunction in June 2026, allowing the law to take effect,

and on July 6, 2026 the Supreme Court denied two emergency applications to block enforcement while the litigation continues [71]. The orders were brief and unsigned, with no noted dissents, and the Court did not reach the First Amendment question, which remains before the Fifth Circuit. The constitutional status of app store accountability laws, including how *Free Speech Coalition v. Paxton* applies to them, therefore remains unsettled.

Policy Recommendations

While the findings in this report confirm some of the concerns that motivated this kind of legislation, they do not establish that app store age verification will stop the harms it intends to prevent. Furthermore, the experience of other states shows that this legislative model continues to evolve (i.e., through litigation, amendment, and delayed implementation). As such, this study does not recommend that the Commonwealth mandate a particular age assurance model at this time, and instead presents the recommendations below.

Make information and tools that already exist trustworthy and usable

Policy options:

- Require app store providers to confirm the accuracy of the age ratings and content descriptions through independent oversight, instead of relying only on the developers' self-assessment. A qualified third party (i.e., neither the app store provider nor the developer) should perform this audit, such as an accredited assessor of the kind approved as a COPPA safe harbor program (e.g., PRIVO, kidSAFE). The audit should cover, for instance, the most downloaded apps, those receiving a threshold number of user complaints about their rating, those that have undergone a significant change, or a random representative sample. App store providers should publish the results and file them with the Attorney General.
- Require that parental controls be usable (i.e., easy to find, configurable, and understandable without technical knowledge). App store providers should demonstrate that these conditions are met through usability testing with a representative sample of parents, publish the results periodically (e.g., annually, monthly) and file them with the Attorney General.
- Require a clear and conspicuous mechanism for users to report inaccurate information (e.g., a wrong age rating, an incomplete content description, or misleading claims about data collection) to the app store provider, and require providers to publish a summary report for this data periodically (e.g., annually, monthly) and file it with the Attorney General. The report should show the volume and category of the received complaints.

Take incremental steps and build in evaluation

Policy options:

- Request verifiable parental consent for downloading or performing a purchase only for those apps whose age rating exceeds the account holder's age category, and for any app involving purchases regardless of the age rating.
- App store providers should provide parent accounts with a centralized dashboard for setting up consent preferences (e.g., granting consent for all apps at or below a given age rating, requiring approval for each individual download, or configuring purchases separately from downloads). The dashboard should be configured to require approval for each covered app by default, with the option for parents to customize those settings [58].
- Require the collection and reporting of data needed to measure whether these requirements work in practice (e.g., number of minor accounts verified, number of parental consent requests issued, granted, and denied, number of downloads or purchases blocked for lack of consent, volume and outcome of complaints received, etc). App store providers should make this information publicly available on their websites and through the app store interface.

Author Information

Alejandro Velasco, Ph.D(c) - Computer Science.
COVES Fellow, William & Mary

Kira Allmann, Ph.D.
Chief Policy Analyst, Joint Commission on Technology & Science

Jodi Kuhn
Executive Director, Joint Commission on Technology & Science

Contact: info@jcots.virginia.gov

Thanks To

Amazon

Computer & Communications Industry Association (CCIA)

Child Safety Advocates

Google

NetChoice

Office of Senator Christopher T. Head

Technet

For providing helpful information and background during the preparation of this report.

References

- [1] Information Security, Cybersecurity and Privacy Protection—Age Assurance Systems—Part 1: Framework, ISO/IEC 27566-1:2025, International Organization for Standardization, Geneva, Switzerland, 1st ed., Dec. 2025. Accessed: Jul. 28, 2026. [Online]. Available: <https://www.iso.org/standard/88143.html>.
- [2] R. Alajaji, “Age verification, estimation, assurance, oh my! A guide to the terminology,” Electronic Frontier Foundation, San Francisco, CA, USA, Oct. 30, 2025. Accessed: Jul. 28, 2026. [Online]. Available: <https://www.eff.org/deeplinks/2025/10/age-verification-estimation-assurance-oh-my-guide-terminology>.
- [3] Utah App Store Accountability Act Amendments, H.B. 498, 2026 Gen. Sess. (Utah 2026) (amending S.B. 142, 2025 Gen. Sess.). Accessed: Jul. 28, 2026. [Online]. Available: <https://le.utah.gov/~2026/bills/static/HB0498.html>.
- [4] Protection of Children on Applications, H.B. 570, Act No. 481, 2025 Reg. Sess. (La. 2025). Accessed: Jul. 28, 2026. [Online]. Available: <https://www.legis.la.gov/legis/BillInfo.aspx?i=248616>.
- [5] App Store Accountability Act, S.B. 2420, 89th Leg., Reg. Sess. (Tex. 2025). Accessed: Jul. 28, 2026. [Online]. Available: <https://capitol.texas.gov/BillLookup/History.aspx?Bill=SB2420&LegSess=89R>.
- [6] App Store Accountability Act, H.B. 161, Act 2026-59 (Ala. 2026). Accessed: Jul. 28, 2026. [Online]. Available: <https://alison.legislature.state.al.us/files/pdf/SearchableInstruments/2026RS/HB161-enr.pdf>.
- [7] K. Hanaoka, M. Ngan, J. Yang, G. W. Quinn, A. Hom, and P. Grother, “Face analysis technology evaluation: Age estimation and verification,” National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST Internal Report NIST IR 8525, May 2024, doi: 10.6028/NIST.IR.8525.
- [8] Google, “Use Play Age Signals API (beta),” Android Developers, updated Jul. 20, 2026. Accessed: Jul. 28, 2026. [Online]. Available: <https://developer.android.com/google/play/age-signals/use-age-signals-api>.

- [9] Samsung Electronics, “Get age signals,” Samsung Developer, 2026. Accessed: Jul. 28, 2026. [Online]. Available: <https://developer.samsung.com/galaxy-store/galaxy-store-content-provider-api/get-age-signals.html>.
- [10] Consumer Data Protection Act, Va. Code Ann. tit. 59.1, ch. 53. Accessed: Jul. 28, 2026. [Online]. Available: <https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/>.
- [11] Data Controller Responsibilities; Transparency, Va. Code Ann. § 59.1-578. Accessed: Jul. 28, 2026. [Online]. Available: <https://law.lis.virginia.gov/vacode/title59.1/chapter53/section59.1-578/>.
- [12] Children’s Online Privacy Protection Rule, 16 C.F.R. pt. 312. Accessed: Jul. 28, 2026. [Online]. Available: <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312>.
- [13] European Commission, “The EU approach to age verification,” Shaping Europe’s Digital Future, updated May 13, 2026. Accessed: Jul. 28, 2026. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification>.
- [14] A. Stapelberg, “Opening up ‘zero-knowledge proof’ technology to promote privacy in age assurance,” Google, Jul. 3, 2025. Accessed: Jul. 28, 2026. [Online]. Available: <https://blog.google/innovation-and-ai/technology/safety-security/opening-up-zero-knowledge-proof-technology-to-promote-privacy-in-age-assurance/>.
- [15] M. Faverio and O. Sidoti, “Teens, social media and technology 2024,” Pew Research Center, Washington, DC, USA, Dec. 12, 2024. Accessed: Jul. 28, 2026. [Online]. Available: <https://www.pewresearch.org/internet/2024/12/12/teens-social-media-and-technology-2024/>.
- [16] U.S. Department of Health and Human Services, “Social media and youth mental health: The U.S. Surgeon General’s advisory,” Office of the Surgeon General, Washington, DC, USA, 2023. Accessed: Jul. 28, 2026. [Online]. Available: <https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf>.
- [17] Centers for Disease Control and Prevention, “Youth risk behavior survey data summary & trends report: 2013–2023,” Atlanta, GA, USA, 2024. Accessed: Jul. 28, 2026. [Online]. Available: <https://www.cdc.gov/yrb/dstr/pdf/YRBS-2023-Data-Summary-Trend-Report.pdf>.
- [18] Common Sense Media, “Teens and pornography,” San Francisco, CA, USA, Jan. 10, 2023. Accessed: Jul. 28, 2026. [Online]. Available: <https://www.commonsensemedia.org/research/teens-and-pornography>.
- [19] Common Sense Media, “Talk, trust, and trade-offs: How and why teens use AI companions,” San Francisco, CA, USA, Jul. 16, 2025. Accessed: Jul. 28, 2026. [Online]. Available: <https://www.commonsensemedia.org/research/talk-trust-and-trade-offs-how-and-why-teens-use-ai-companions>.
- [20] Federal Trade Commission, “FTC launches inquiry into AI chatbots acting as companions,” Washington, DC, USA, Sep. 11, 2025. Accessed: Jul. 28, 2026. [Online]. Available: <https://www.ftc.gov/news-events/news/press-releases/2025/09/ftc-launches-inquiry-ai-chatbots-acting-companions>.
- [21] Federal Trade Commission, “Mobile apps for kids: Disclosures still not making the grade,” FTC Staff Report, Washington, DC, USA, Dec. 2012. Accessed: Jul. 28, 2026. [Online]. Available:

<https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-disclosures-still-not-making-grade/121210mobilekidsappreport.pdf>.

[22] Federal Trade Commission, “Mobile apps for kids: Current privacy disclosures are disappointing,” FTC Staff Report, Washington, DC, USA, Feb. 2012. Accessed: Jul. 28, 2026. [Online]. Available: https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf.

[23] R. Sun, M. Xue, G. Tyson, S. Wang, S. Camtepe, and S. Nepal, “Not seen, not heard in the digital world! Measuring privacy practices in children’s apps,” in Proceedings of the ACM Web Conference 2023 (WWW ’23), Austin, TX, USA, Apr.–May 2023, pp. 2166–2177, doi: 10.1145/3543507.3583327.

[24] F. Yu, F. Xie, N. Dong, and G. Bai, “A large-scale analysis of privacy labels in child-accessible mobile applications,” in Advanced Data Mining and Applications (ADMA 2025), Lecture Notes in Computer Science, vol. 16198. Singapore: Springer, 2026, pp. 461–469, doi: 10.1007/978-981-95-3456-2_32.

[25] Federal Trade Commission, “Apple Inc. will provide full consumer refunds of at least \$32.5 million to settle FTC complaint it charged for kids’ in-app purchases without parental consent,” Washington, DC, USA, Jan. 15, 2014. Accessed: Jul. 28, 2026. [Online]. Available: <https://www.ftc.gov/news-events/news/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million-settle-ftc-complaint-it-charged-kids>.

[26] Federal Trade Commission, “Fortnite refunds,” Washington, DC, USA. Accessed: Jul. 28, 2026. [Online]. Available: <https://www.ftc.gov/enforcement/refunds/fortnite-refunds>.

[27] Federal Trade Commission, “FTC staff report finds large social media and video streaming companies have engaged in vast surveillance of users with lax privacy controls and inadequate safeguards for kids and teens,” Washington, DC, USA, Sep. 19, 2024. Accessed: Jul. 28, 2026. [Online]. Available: <https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-staff-report-finds-large-social-media-video-streaming-companies-have-engaged-vast-surveillance>.

[28] Apple, “Age requirements for apps distributed in Brazil, Australia, Singapore, Utah, and Louisiana,” Apple Developer News, Feb. 24, 2026. Accessed: Jul. 28, 2026. [Online]. Available: <https://developer.apple.com/news/?id=f5zj08ey>.

[29] Amazon, “User age verification,” Appstore Developer Documentation, updated Jul. 17, 2026. Accessed: Jul. 28, 2026. [Online]. Available: <https://developer.amazon.com/docs/app-submission/user-age-verification.html>.

[30] Google, “Changes to Google Play for upcoming app store bills for users in applicable US states,” Play Console Help, updated Oct. 9, 2025. Accessed: Jul. 28, 2026. [Online]. Available: <https://support.google.com/googleplay/android-developer/answer/16569691>.

[31] Apple, “New requirements for apps available in Texas,” Apple Developer News, Oct. 8, 2025. Accessed: Jul. 28, 2026. [Online]. Available: <https://developer.apple.com/news/?id=btkirlj8>.

- [32] M. Anderson, M. Faverio, and E. Park, “How teens and parents approach screen time,” Pew Research Center, Washington, DC, USA, Mar. 11, 2024. Accessed: Jul. 28, 2026. [Online]. Available: <https://www.pewresearch.org/internet/2024/03/11/how-teens-and-parents-approach-screen-time/>.
- [33] E. Rescorla, Z. Arnao, and A. Cooper, “Age assurance online: A technical assessment of current systems and their limitations,” Knight-Georgetown Institute, Washington, DC, USA, Jan. 29, 2026. Accessed: Jul. 28, 2026. [Online]. Available: <https://kgi.georgetown.edu/research-and-commentary/age-assurance-online/>.
- [34] Google, “Content rating requirements for apps, games, and the ads served on both,” Play Console Help, updated 2026. Accessed: Jul. 28, 2026. [Online]. Available: <https://support.google.com/googleplay/android-developer/answer/9859655>.
- [35] International Age Rating Coalition, “Frequently asked questions,” IARC. Accessed: Jul. 28, 2026. [Online]. Available: <https://globalratings.com/faq/>.
- [36] Apple, “Updated age ratings in App Store Connect,” Apple Developer News, Jul. 24, 2025. Accessed: Jul. 28, 2026. [Online]. Available: <https://developer.apple.com/news/?id=ks775ehf>.
- [37] D. Denipitiyage, B. Silva, K. Gunathilaka, S. Seneviratne, A. Mahanti, A. Seneviratne, and S. Chawla, “Detecting and characterising mobile app metamorphosis in Google Play Store,” *IEEE Transactions on Mobile Computing*, vol. 24, no. 8, pp. 7489–7504, Aug. 2025, doi: 10.1109/TMC.2025.3550121.
- [38] S. Lavermicocca, M. Carminati, and S. Longari, “X-rated compliance theater: An empirical evaluation of European age verification systems in adult websites,” *arXiv:2606.08667*, Jun. 2026, doi: 10.48550/arXiv.2606.08667.
- [39] *Computer & Communications Industry Association v. Paxton*, No. 1:25-cv-01660-RP (W.D. Tex. Dec. 23, 2025) (order granting preliminary injunction), consolidated with *Students Engaged in Advancing Texas v. Paxton*, No. 1:25-cv-01662 (W.D. Tex.). Accessed: Jul. 28, 2026. [Online]. Available: <https://storage.courtlistener.com/recap/gov.uscourts.txwd.1172869998/gov.uscourts.txwd.1172869998.65.0.pdf>.
- [40] New America, “App stores vs. platforms: Who should be verifying Internet users’ ages?,” New America, Washington, DC, USA, 2026. Accessed: Jul. 28, 2026. [Online]. Available: <https://www.newamerica.org/insights/app-stores-vs-platforms-who-should-be-verifying-internet-users-ages/>.
- [41] Google, “Alternative distribution options,” Android Developers, updated 2026. Accessed: Jul. 28, 2026. [Online]. Available: <https://developer.android.com/distribute/marketing-tools/alternative-distribution>.
- [42] D. Lang, B. Listyg, B. V. Ross, A. V. Musquera, and Z. Sanderson, “Age verification and public adaptation: A pre-registered synthetic control multiverse,” *Journal of Law & Empirical Analysis*, vol. 3, no. 1, pp. 23–50, Jun. 2026, doi: 10.1177/2755323X251415424.
- [43] Australian Government, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, “Age assurance technology trial—Part D: Age estimation,” Canberra, ACT, Australia, 2025. Accessed: Jul. 28, 2026. [Online]. Available: https://ageassurance.com.au/wp-content/uploads/2025/08/AATT_Part_D_DIGITAL.pdf.

- [44] Age Assurance Technology Trial, “Final report,” 2025. Accessed: Jul. 28, 2026. [Online]. Available: <https://ageassurance.com.au/report/>.
- [45] Age Assurance Technology Trial, “Case studies,” 2025. Accessed: Jul. 28, 2026. [Online]. Available: <https://ageassurance.com.au/case-studies/>.
- [46] C. Barnes et al., “Assessing early effects of Australia’s Social Media Minimum Age Act on adolescents’ social media use: Observational study,” *BMJ*, vol. 393, Art. no. e363695, Jun. 2026, doi: 10.1136/bmj-2026-363695.
- [47] Molly Rose Foundation, “Australia’s social media ban—is it working?,” London, U.K., Apr. 2026. Accessed: Jul. 28, 2026. [Online]. Available: https://mollyrosefoundation.org/wp-content/uploads/2026/04/MRF_Australia-Social-Media-Ban-Research_Briefing-April-26.pdf.
- [48] R. Speed, “UK VPN demand soars after debut of Online Safety Act,” *The Register*, Jul. 28, 2025. Accessed: Jul. 28, 2026. [Online]. Available: <https://www.theregister.com/2025/07/28/uk-vpn-demand-soars-after-debut-of-online-safety-act/>.
- [49] B. Nansen, H. Sandberg, L. Bliss, and S. Cohny, “From phreaking to sneaking: Children’s circumvention of social media age verification systems,” arXiv:2605.00368, May 2026, doi: 10.48550/arXiv.2605.00368.
- [50] S. Basu, “Facial age estimation,” Parliamentary Office of Science and Technology, London, U.K., Rapid Response RR106, Jul. 16, 2026, doi: 10.58248/RR106.
- [51] New America, “Challenges with age verification,” in *Age Verification: The Complicated Effort to Protect Youth Online*, New America, Washington, DC, USA, Jan. 2026. Accessed: Jul. 28, 2026. [Online]. Available: <https://www.newamerica.org/insights/age-verification-the-complicated-effort-to-protect-youth-online/challenges-with-age-verification/>.
- [52] M. Rasch, “When privacy laws force you to know too much: The perverse incentives of age verification regimes,” *Security Boulevard*, Apr. 10, 2026. Accessed: Jul. 28, 2026. [Online]. Available: <https://securityboulevard.com/2026/04/when-privacy-laws-force-you-to-know-too-much-the-perverse-incentives-of-age-verification-regimes/>.
- [53] A. A. Johnson Ash, “Age-appropriate design codes are just age verification in disguise,” Information Technology & Innovation Foundation, Washington, DC, USA, May 24, 2024. Accessed: Jul. 28, 2026. [Online]. Available: <https://itif.org/publications/2024/05/24/age-appropriate-design-codes-are-age-verification-in-disguise/>.
- [54] Discord, “Update on a security incident involving third-party customer service,” Discord Press Releases, Oct. 3, 2025, updated Oct. 9, 2025. Accessed: Jul. 28, 2026. [Online]. Available: <https://discord.com/press-releases/update-on-security-incident-involving-third-party-customer-service>.
- [55] UNICEF, “Age restrictions alone won’t keep children safe online,” UNICEF Press Centre, New York, NY, USA, Dec. 9, 2025. Accessed: Jul. 28, 2026. [Online]. Available: <https://www.unicef.org/press-releases/age-restrictions-alone-wont-keep-children-safe-online>.

- [56] A. Abdallah, A. Ahmad, and B. Said, “Balancing privacy and usability: A design science research approach for cookie consent mechanisms,” *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 11, no. 2, Art. no. 100520, Jun. 2025, doi: 10.1016/j.joitmc.2025.100520.
- [57] European Commission, “Digital package,” *Shaping Europe’s Digital Future*, Nov. 20, 2025. Accessed: Jul. 28, 2026. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/faqs/digital-package>.
- [58] Family Online Safety Institute, “Parental controls for online safety are underutilized, new study finds,” *Family Online Safety Institute*, Washington, DC, USA, May 28, 2025. Accessed: Jul. 28, 2026. [Online]. Available: <https://fosi.org/parental-controls-for-online-safety-are-underutilized-new-study-finds/>.
- [59] P. Wisniewski, A. K. Ghosh, H. Xu, M. B. Rosson, and J. M. Carroll, “Parental control vs. teen self-regulation: Is there a middle ground for mobile online safety?,” in *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW ’17)*, Portland, OR, USA, Feb. 2017, pp. 51–69, doi: 10.1145/2998181.2998352.
- [60] K. Badillo-Urquiola, C. Chouhan, S. Chancellor, M. De Choudhury, and P. Wisniewski, “Beyond parental control: Designing adolescent online safety apps using value sensitive design,” *Journal of Adolescent Research*, vol. 35, no. 1, pp. 147–175, Jan. 2020, doi: 10.1177/0743558419884692.
- [61] A. K. Ghosh, K. Badillo-Urquiola, M. B. Rosson, H. Xu, J. M. Carroll, and P. J. Wisniewski, “A matter of control or safety? Examining parental use of technical monitoring apps on teens’ mobile devices,” in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI ’18)*, Montreal, QC, Canada, Apr. 2018, pp. 1–14, doi: 10.1145/3173574.3173768.
- [62] App Store Accountability Act, S.B. 237, 2026 Reg. Sess. (Va. 2026). Accessed: Jul. 28, 2026. [Online]. Available: <https://lis.virginia.gov/bill-details/2026/SB237>.
- [63] App Store Accountability Act, H.B. 757, 2026 Reg. Sess. (Va. 2026) (continued to 2027 Sess.). Accessed: Jul. 28, 2026. [Online]. Available: <https://lis.virginia.gov/bill-details/2026/HB757>.
- [64] App Store Accountability Act, S. 1586, 119th Cong. (2025). Accessed: Jul. 28, 2026. [Online]. Available: <https://www.congress.gov/bill/119th-congress/senate-bill/1586>.
- [65] App Store Accountability Act, H.R. 3149, 119th Cong. (2025). Accessed: Jul. 28, 2026. [Online]. Available: <https://www.congress.gov/bill/119th-congress/house-bill/3149>.
- [66] Digital Age Assurance Act, A.B. 1043, 2025–2026 Reg. Sess. (Cal. 2025). Accessed: Jul. 28, 2026. [Online]. Available: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260AB1043.
- [67] Age Attestation on Computing Devices, S.B. 26-051, 75th Gen. Assemb., 2d Reg. Sess. (Colo. 2026). Accessed: Jul. 28, 2026. [Online]. Available: <https://leg.colorado.gov/bills/SB26-051>.
- [68] Louisiana Legislature, H.B. 977, 2026 Reg. Sess. (La. 2026) (delaying and reenacting Act No. 481). Accessed: Jul. 28, 2026. [Online]. Available: <https://legis.la.gov/legis/BillInfo.aspx?i=251085>.

[69] Application Stores, S.B. 1722, 2026 Reg. Sess. (Fla. 2026). Accessed: Jul. 28, 2026. [Online]. Available: <https://www.flsenate.gov/Session/Bill/2026/1722/>.

[70] Free Speech Coalition, Inc. v. Paxton, 606 U.S. __, No. 23-1122 (U.S. Jun. 27, 2025). Accessed: Jul. 28, 2026. [Online]. Available: https://www.supremecourt.gov/opinions/24pdf/23-1122_3e04.pdf.

[71] Students Engaged in Advancing Texas v. Paxton, No. 25A1389, and Computer & Communications Industry Association v. Paxton, No. 25A1390 (U.S. Jul. 6, 2026) (applications to vacate stay denied). Accessed: Jul. 28, 2026. [Online]. Available: <https://www.supremecourt.gov/docket/docketfiles/html/public/25a1389.html>.

[72] eSafety Commissioner, “Social media minimum age—regulatory guidance,” Australian Government, Sep. 16, 2025. Accessed: Jul. 30, 2026. [Online]. Available: <https://www.esafety.gov.au/sites/default/files/2025-09/eSafety-SMMA-Regulatory-Guidance.pdf>.