

CHILDREN'S PRIVACY AND APP STORE ACCOUNTABILITY: **THE RISKS OF KNOWING TOO MUCH**



BY JUSTIN YEDOR



& TUCKER SARCHIO

Justin Yedor is a data privacy lawyer and a Partner at BakerHostetler LLP. Justin helps his clients to develop creative solutions to data privacy challenges. He is a thought leader on California privacy law and a go-to advisor on the California Consumer Privacy Act (CCPA) and the next wave of U.S. state privacy laws taking effect across the country. Tucker Sarchio is a data privacy lawyer and an Associate at BakerHostetler LLP. Tucker advises clients on all aspects of compliance with U.S. state and federal privacy laws.

TechREG CHRONICLE FEBRUARY 2026

THE DIGITAL FAIRNESS ACT: A NEW LAYER IN THE EU'S DIGITAL RULEBOOK?
By Christelle Coslin & Hicham Kaddoum

TAKING THE CON OUT OF CONSUMER PROTECTION: MATERIALITY AND INJURY IN ONLINE DISCLOSURE CASES
Michael R. Baye, Nathan Blalock & R. Andrew Butters

DIGITAL FAIRNESS ACT: A PATHBREAKER FOR EU DIGITAL CONSUMER LAW
By Philip Andrews & Aleksandra Pruska

ONLINE CONSUMER PROTECTION: SOME PERSPECTIVES FROM LAW AND ECONOMICS
By Julian Morris

CHILDREN'S PRIVACY AND APP STORE ACCOUNTABILITY: THE RISKS OF KNOWING TOO MUCH
By Justin Yedor & Tucker Sarchio

Visit www.competitionpolicyinternational.com for access to these articles and more!

CHILDREN'S PRIVACY AND APP STORE ACCOUNTABILITY: THE RISKS OF KNOWING TOO MUCH

By Justin Yedor & Tucker Sarchio

Children's privacy and online protections have taken center stage among legislators and regulators worldwide. In the United States, states are rapidly scaling up regulation of children's privacy and online safety. This article discusses how recently enacted app store accountability laws are intersecting with state comprehensive privacy laws, upending strategies many businesses have used to comply with older children's privacy laws and minimize their data collection. The article will explore the tension and intersection of these legal regimes, a recent constitutional challenge, and practical steps for compliance in light of the uncertain regulatory environment.

Scan to Stay Connected!

Scan here to subscribe to CPI's **FREE** daily newsletter.

01
INTRODUCTION

One of the foundational principles of data privacy compliance is the concept of data minimization, or the idea that the collection of personal data should be limited to what is necessary for the purposes for which data are processed.[2] For years, businesses have found that avoiding the collection of consumers' ages not only advances the principle of data minimization but also substantially simplifies their privacy compliance. Now, a new wave of U.S. state laws is mandating that they collect information indicating the age of their app users and raising significant questions about the impact on consumers' privacy.

Currently, 19 U.S. states have enacted comprehensive privacy laws, each of which includes some level of protection for children's personal data. Increasingly, these laws impose consent requirements, or outright bans, on sales of personal data and targeted advertising to children and teens. These restrictions generally apply to businesses that have "actual knowledge" or "willfully disregard" the age of the consumer they interact with. While these restrictions may sound thorny, many businesses are not subject to them because they do not collect information about individual users' ages, either because they do not need that data, as a strategy to avoid these requirements, or both.

An additional set of laws passed over the last year is now challenging this strategy. In 2025, California, Louisiana, Texas, and Utah passed laws requiring app stores to take affirmative steps to verify the age of their users, obtain and track parental consent tied to downloads and inapp purchases, and provide developers with user age data (collectively, the "App Store Accountability Laws" or "ASA Laws"). As a result, businesses that carefully avoided the collection of user ages may soon find themselves in possession of this data, opening up a host of new compliance challenges.

02
BACKGROUND — FEDERAL AND STATE LAWS PROTECTING CHILDREN'S PRIVACY

Since the Children's Online Privacy Protection Act ("COPPA") took effect in 2000, many companies that provide online services for a general audience have complied in large part by avoiding the collection of data about their users' ages. This worked because the core requirements of COPPA apply only to companies that have "actual knowledge" that they are collecting, using, or disclosing personal data from children under 13.[3] If a restaurant, online retailer, or other business whose website or app is intended for a general audience does not specifically direct its service to children and can avoid actual knowledge about website and app users' ages, the business can largely avoid obligations under COPPA.

As newer laws like the California Consumer Privacy Act ("CCPA"), the Texas Data Privacy and Security Act ("TDPSA"), and other state comprehensive privacy laws took effect, they too imposed special protections for children's personal data — particularly for practices such as targeted advertising, so-called "sales" of personal data,[4] and

2 See Regulation (EU) 2016/679 (General Data Protection Regulation), art. 5(1)(c) ("Personal data shall be . . . adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').").

3 "Actual knowledge" is not neatly defined under COPPA but can arise in various contexts such as: (1) when a user of an online service who is under 13 provides their age directly; (2) when another party, such as a parent or guardian, indicates that a user of an online service is under 13; and (3) when an online service is "directed to children," based on a variety of factors, including "subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the website or online service, as well as whether advertising promoting or appearing on the website or online service is directed to children." 16 CFR § 312.2.

4 "Targeted advertising" is defined as "displaying to a consumer an advertisement that is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests." 11 Tex. Bus. & Com. Code § 541.001(31). A "sale" of personal data under these types of privacy laws often includes "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or *other valuable consideration*." Cal. Civ. Code § 1798.140(ad)(1) (emphasis added); 11 Tex. Bus. & Com. Code § 541.001(28) (defining a "sale" as "sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party").

© 2026 Competition Policy International All Rights Reserved

profiling. The CCPA, for example, provides that a business may not sell the personal data of a consumer under 16 or share it for cross-context behavioral advertising without first obtaining opt-in consent if the business has "actual knowledge" of the consumer's age.[5] If the consumer is known to be under 13, the business must obtain consent from the parent.[6] These rules contrast with the CCPA's requirements for adults, which require only that businesses provide an after-the-fact opt-out from sales of personal data and cross-context behavioral advertising.

The TDPSA and several other state privacy laws classify personal data collected from a "known child" under 13 as sensitive—meaning that a business must obtain prior opt-in consent from the parent before processing such data for *any* purpose.[7] If a business subject to the TDPSA "sells" sensitive personal data (including personal data about a known child), it must provide consumers with a notice stating "NOTICE: We may sell your sensitive personal data."[8] However, these special rules for children's data under the TDPSA still only apply "where a controller has actual knowledge of, or wilfully disregards, the child's age."[9]

Some states have started to loosen the "actual knowledge" standard while imposing further restrictions on targeted advertising and sales of personal data of minors. For example, Delaware requires opt-in consent for targeted advertising and sales of personal data about a consumer under 18.[10] Maryland took this a step further, imposing an outright ban on targeted advertising and sales of personal data "if the controller knew or should have known" that the consumer is under 18.[11] Some states that already had comprehensive privacy laws, such as Colorado and Oregon, have recently amended their laws to add these new types of restrictions.[12]

03

THE EVOLVING LEGAL LANDSCAPE — APP STORE ACCOUNTABILITY LAWS

In 2025, California, Louisiana, Texas, and Utah passed the App Store Accountability Laws, intending to limit minors' exposure to inappropriate content and practices via mobile apps.[13] The ASA Laws regulate both app stores and app developers. While the specifics vary somewhat, the Texas, Utah, and Louisiana ASA Laws generally require app stores to:

- Verify user age at account creation in order to distinguish minors from adult users.
- Classify minor accounts into specific age brackets: children (under 13), younger teens (13–15), older teens (16–17), and adults (18+).
- Obtain parental consent for app downloads, app purchases, and in-app purchases by minors.

The California law is similar but includes technical obligations not found in the other three ASA Laws. For example, under the California ASA Law, app stores must provide an accessible interface for users to indicate their age at ac-

5 Cal. Civ. Code § 1798.120(c).

6 *Ibid.*

7 11 Tex. Bus. & Com. Code § 541.001(29); *id.* § 541.101(b)(4).

8 *Ibid.* § 541.102(b).

9 *Ibid.* § 541.001(17).

10 6 Del. Code § 12D-106(a)(7).

11 Md. Code Ann., Com. Law § 14-4607(A)(4)–(5).

12 Or. H.B. 2008, 82d Leg. Assemb., Reg. Sess. (2025); Colo. S.B. 24041, 74th Gen. Assemb., Reg. Sess. (2024).

13 Tex. Bus. & Com. Code §§ 121.001 *et seq.*; La. Rev. Stat. §§ 51:1771 *et seq.*; Utah Code §§ 1376101 *et seq.*; Cal. A.B. 1043 2025–2026 Leg., Reg. Sess. (2025).
The California law also covers operating system providers. For simplicity, this article focuses on mobile apps.
The California ASA Law is slated to take effect January 1, 2027. The Texas ASA Law was supposed to take effect January 1, 2026, but is currently subject to a preliminary injunction as discussed in more detail below. The Utah ASA Law will take effect on May 6, 2026, and the Louisiana ASA Law will take effect on July 1, 2026.

© 2026 Competition Policy International® All Rights Reserved

count setup and must provide app developers with a signal containing the user's age bracket via APIs.[14]

For their part, app developers must:

- Publish an age rating for their apps according to the age brackets established by the app stores.
- Verify age and consent through the app store, including receiving information about the user's age or age bracket.
- Notify the app store of a "significant change" to an app, such as those relating to material modification of the app's terms of service, privacy policy, content or age rating, monetization features, or user experience.
- Request personal age verification data or parental consent when a user downloads or purchases an app, or when implementing a "significant change" to an app, per the Utah and Louisiana ASA Laws.

Based on Apple's and Google's proposed implementation of their obligations under the ASA Laws, it is assumed that the app stores will only provide age data about users in a specific covered state and do not plan to voluntarily roll out this type of age verification for all states.

04
DISCUSSION

Curiously, in the interest of protecting minors, the ASA Laws specifically require businesses to receive personal data they might otherwise never collect. For example, a retail business that develops an app with content appropriate for all ages might soon find itself in possession of information stating that specific app users are under 13, between 13 and 15, or between 16 and 17, or even the exact age of a specific user. Collecting any of this information about a user's age is likely to trigger an obligation to comply with COPPA if it shows the user is under 13 because the age data received from an app store is likely to provide the business with "actual knowledge" of the user's age. Additionally, under laws like the TDPSA, all personal data associated with that user would be considered sensitive and therefore subject to additional restrictions and requirements.

Businesses that "sell" personal data or use it for targeted advertising might find themselves facing additional challenges. If the business uses personal data collected through its mobile app for targeted advertising or discloses the data to third parties in ways that count as a "sale" under the comprehensive state privacy laws, it will need to build an opt-in consent mechanism for the app. In the mobile app context, honoring consent requirements can be tricky. For example, while managing cookie consents on websites has become common practice, the ability to offer in-app consent management is still relatively underdeveloped. Businesses may not have a full picture of the software development kits ("SDKs") running in their apps and may not have a tool to opt children out of SDKs that constitute a sale, sharing, or targeted advertising under state privacy laws.

All of this poses challenges not only for a mobile app itself but also for other services offered by the business, including its website. If a mobile app allows users to create an account that can be accessed via the web, businesses may also be found to have actual knowledge of a user's age when the user logs into their account on the website. Even if the user does not log in, a regulator could argue that the prevalence of users under 18 on a mobile app means the business "should know" that it has users under 18 on its website. While this may not meet the "actual knowledge" standard found in many state privacy laws, it is at least a plausible argument and has not yet been tested in this context. A business that fails to obtain opt-in consent or disable targeted advertising trackers when an app user of minor age visits its website could be found to be willfully disregarding user age.

In light of these challenges, some businesses are likely to rate their mobile applications as 18+ so as to avoid the collection of personal data about minors. Although this may be a perfectly rational business decision, it is unfortunate because it would result in reduced availability of mobile applications for users under 18 — more on these concerns below in the discussion of the recent preliminary injunction preventing the Texas ASA Law from taking effect. For many apps, though, an 18+ rating is simply not feasible from a business perspective because teen users may be an important part of the app's user base. Companies that operate these apps will need to factor in additional compliance steps involving everything from ensuring that content is appropriate to the age of the user to compliance with the consent, advertising, and sale restrictions applicable to minors under the state privacy laws.

Although at present, ASA laws have only been enacted in four states, businesses that become aware of a meaningful number of under-18 app users in those states may not be immune to regulatory scrutiny in other states with comprehensive privacy laws. For example, it is not difficult to imagine that a Maryland regulator might conclude that if an app developer becomes aware that a portion of its users in

14 Both Apple and Google have released tools designed to assist app developers in complying with their obligations under ASA Laws, including by implementing an application programming interface ("API") that allows the app store to transmit user age data to the developer.

© 2026 Competition Policy International® All Rights Reserved

California, Louisiana, Texas, or Utah are under 18, the "controller knew or should have known" that there were also Maryland consumers under 18 who use the app, meaning that the controller would need to avoid targeted advertising or sales of personal data relating to those users. In short, although ASA Laws have been enacted in only four states, the implications could extend to many other states with laws protecting children's privacy.

05

CONSTITUTIONAL CHALLENGE — WILL THE ASA LAWS ACTUALLY TAKE EFFECT?

The discussion above is likely to raise questions regarding compelled speech and teens' potential loss of access to apps, some of which could include services like news apps or e-books. On December 23, 2025, a federal court in Texas granted the Computer & Communications Industry Association's ("CCIA") motion for a preliminary injunction against the Texas ASA Law, finding that the law likely violates the First Amendment to the U.S. Constitution.[15] Reviewing the requirements for age verification, parental consent, displaying state-mandated age ratings, and restricting access to apps and in-app content based on those ratings, the court concluded that the Texas ASA Law is a content-based regulation because it applies differently depending on the type of speech an app provides and seeks to shield minors from speech the state deems harmful. Applying strict scrutiny, the court found that Texas failed to demonstrate a compelling interest for restricting minors' access to nearly all apps and that the law was not narrowly tailored, especially given its sweeping scope, its over- and under-inclusiveness, and the availability of less restrictive alternatives.

Separately, the court held that key provisions of the Texas ASA Law are unconstitutionally vague, including requirements that developers assign state-mandated age ratings without clear standards and provide notice of undefined "material changes." These vague requirements risk arbitrary enforcement and incentivize over-censorship, further burdening protected speech. Because the law's unconstitutional applications vastly outweigh any potentially valid ones, the court found it facially invalid and non-severable. Having also determined that the CCIA established irreparable harm and that the balance of equities and public interest favored relief, the court issued a preliminary injunction barring enforcement of the Texas ASA Law, pending resolution of the CCIA's lawsuit.

Although the order on the Texas ASA Law is merely a preliminary injunction and not a final determination, given the similarities between the Texas ASA Law and the ASA Laws in the other three states, it is likely that those laws are also vulnerable to arguments of unconstitutionality. Ultimately, it remains to be seen whether the court will permanently enjoin the Texas ASA Law and whether the other three ASA Laws may be subject to similar challenges.

06

PRACTICAL CONSIDERATIONS — WHAT SHOULD BUSINESSES DO NOW?

The ASA Laws are written with a seemingly limited scope, but by forcing the collection of age information, they combine with other laws to substantially expand the restrictions on data processing via mobile apps and beyond. If these laws end up taking effect as drafted, it will no longer be the case that businesses can avoid "actual knowledge" of a user's age simply by avoiding asking them about it. While businesses await the outcome of the constitutional challenge to the Texas ASA Law, there are steps they should consider to prepare for the ASA Laws taking effect.

First, businesses should identify where their users are located and which ASA and privacy regimes apply. They should also determine an appropriate age rating for their apps and be prepared to ingest app store age and consent signals, turn off targeted advertising for minors, log consent events, and respond to consent revocations.

Second, businesses should assess the downstream impacts that collection of specific user age information may have. These could range from COPPA compliance to additional compliance obligations under the TDPSA, the CCPA, and the Utah Consumer Privacy Act. There may also be impacts in other states with comprehensive privacy laws, particularly in states like Maryland that do not require actual knowledge of a user's age before child-specific privacy restrictions kick in. And businesses should consider how they will implement compliance steps for services beyond

15 See *Computer & Comms. Indus. Ass'n v. Paxton*, No. 1:25-cv-1660 (W.D. Tex. Dec. 23, 2025).

© 2026 Competition Policy International® All Rights Reserved

mobile apps. While it has not been a main focus of this article, the California ASA Law directly applies to "operating system providers," not just app stores. Moreover, if an app user known to be under 18 logs into a company's website, it could necessitate special compliance for the website in addition to the mobile app.

07
CONCLUSION

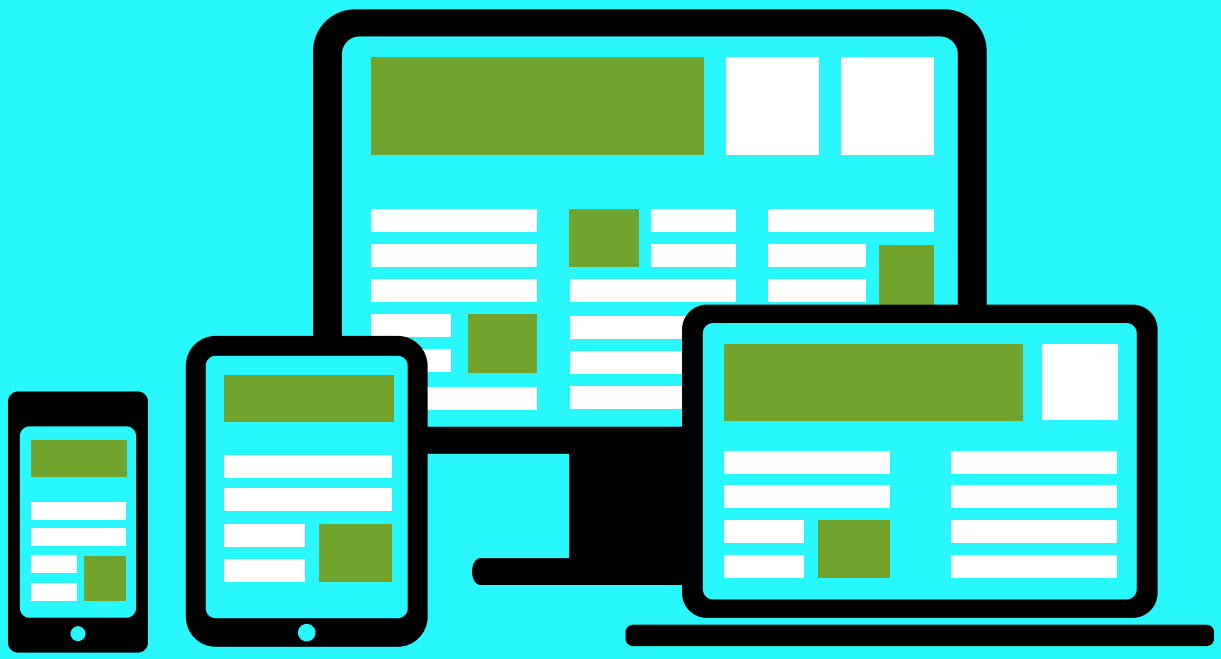
Businesses would be wise to think of the ASA Laws and comprehensive state privacy laws as two components of a single compliance program. While we expect to see continued litigation over the constitutionality of the ASA Laws, the momentum is clearly in favor of heightened protections for children and teens and lowered knowledge standards for businesses. Privacy programs should be designed with this in mind and be flexible enough to adjust to a rapidly evolving landscape.

© 2026 Competition Policy International® All Rights Reserved

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.



© 2026 Competition Policy International® All Rights Reserved

CPI COMPETITION POLICY® INTERNATIONAL