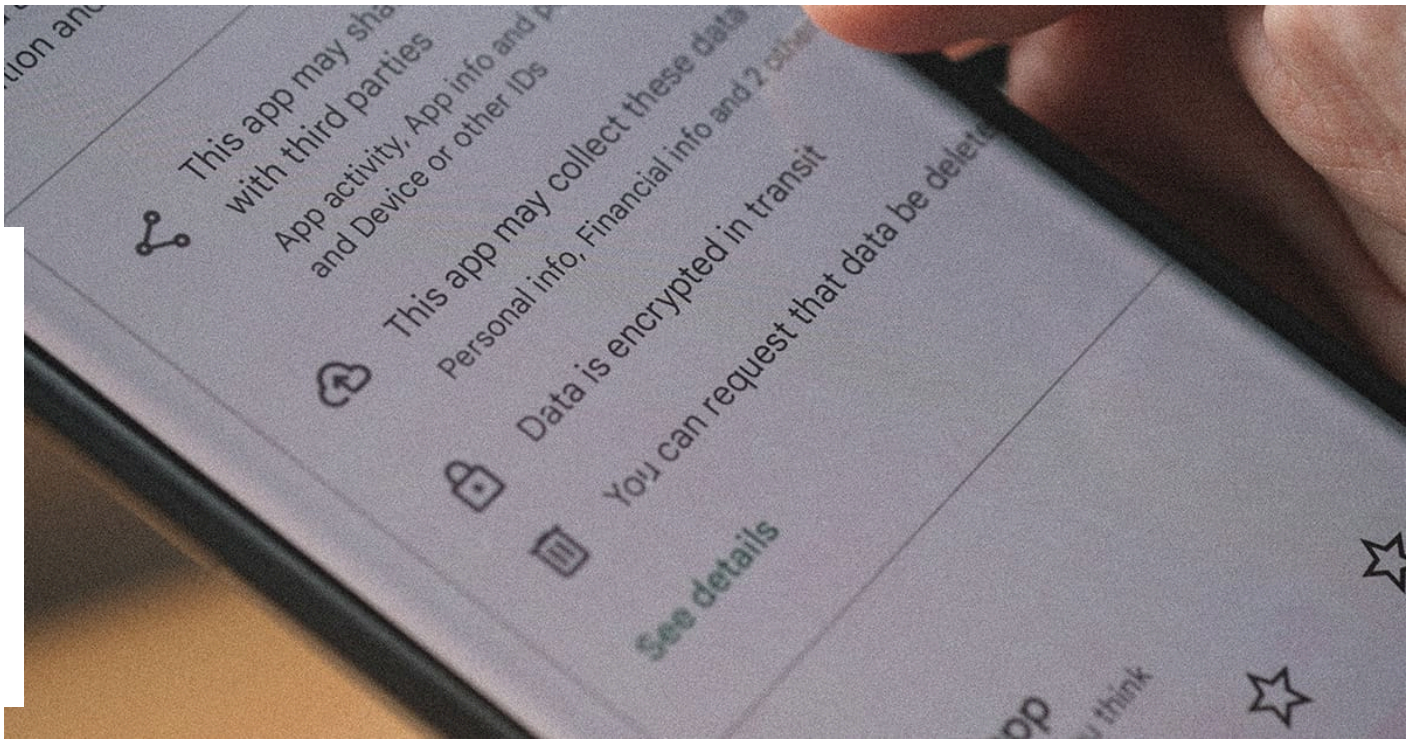
What Companies Need to Know About the Evolving Youth Privacy Landscape

With numerous state youth data laws passed and more in the works, count on a patchwork adding to compliance requirements

by Greg Szewczyk and Madison Etherington — August 10, 2026 in Data Privacy



There is no single compliance model for handling minors' data, but companies can take several steps now to mitigate the risks, attorneys Greg Szewczyk and Madison Etherington of Ballard Spahr explain.

For years, many companies treated youth's privacy on their apps as a narrow compliance question: Is the app directed to users under 13 years old, or does the company have actual knowledge a user is younger than 13?

The federal Children's Online Privacy Protection Act (COPPA) remains a cornerstone for children's privacy compliance, but state laws are rapidly joining and expanding the scope of efforts to regulate how businesses collect, use and share young people's personal information online. App store accountability measures add yet another layer by introducing new evaluation and notice requirements governing methods by which companies receive age-related information.

As a result, businesses are being forced to review the way they collect and process information of users.

COPPA applies to operators of websites and online services directed to youths under 13 as well as those that have actual knowledge that they collect personal information from someone under 13. Covered operators must provide notice and obtain verifiable parental consent before collecting, using or disclosing such data.

This baseline, however, is evolving. The FTC finalized COPPA Rule amendments in 2025 that, among other changes, require separate parental opt-in consent before certain disclosures of youths' personal information to third parties for targeted advertising.

In general, businesses should continue to treat COPPA as a floor for compliance, generally disclosing that products or services are not directed at children and that information will not be collected from children without first obtaining verifiable parental consent. In the event a company becomes aware of the inadvertent collection of children's information, it should be immediately remediated by deleting the information and ceasing all related processing.

However, while COPPA has been the baseline governing processing of children's information for years, a growing number of state privacy laws are beginning to regulate data belonging to teenagers separately.

Teen data is becoming its own compliance category

Several states have begun to enact laws that require businesses to treat the data of individuals between 13 and 18 differently.

- New York's Child Data Protection Act regulates personal data belonging to covered users under 18. For users 13-17 years old, certain processing must either be strictly necessary for specified activities or supported by informed consent. The law also limits some uses of personal data collected while a user was a minor after the user becomes an adult.
- Maryland's Online Data Privacy Act prohibits targeted advertising and the sale of personal data involving consumers whom an organization knew or should have known were under 18.

- Arkansas' Children and Teens' Online Privacy Protection Act creates different obligations relating separately to children below 13 and teens ages 13-16 when a company has actual knowledge it collects their personal information.
- Colorado's Privacy Act was recently amended to provide additional protections over the data of children under 18 when a controller has actual knowledge or willfully disregards information that establishes that a user is a minor, and the Department of Law has rulemaking authority. In the draft rules that have been published, the attorney general lists factors that should be considered when determining whether a controller has willfully disregarded whether a consumer is a minor. Those factors include if the user can provide their age, if the user can edit their age, if the user has a bio section of a profile, if there is indicia of age, such as grade level, and if the company categorizes them differently for marketing purposes. However, the draft rules expressly state that the list is not exhaustive, and the determination will be based on the totality of the circumstances.

Because of this breadth of legislation, companies face highly granular questions: When does it make sense — or become mandatory — to disable targeted advertising altogether? To limit third-party sharing? To restrict social features? In some situations, creating dedicated interfaces just for minors might offer the simplest path forward.

Along with the US, Canada's approach is continuing to develop. In May 2026, the Office of the Privacy Commissioner of Canada released guidance advising organizations to assess whether age assurance is necessary, use methods proportionate to the risks involved and consider alternatives, such as limiting certain data practices or turning them off by default.

Canada's Personal Information Protection and Electronic Documents Act requires meaningful consent before organizations collect, use or disclose any individual's personal information. Canadian guidance says parental/guardian permission is needed below age 13, while older minors' maturity level matters more than simple birthdate cutoff. Quebec goes further, barring collection directly from minors under 14 years old without parent or tutor permission unless the collection is clearly for the minor's benefit.

Ultimately, companies should not assume that one national policy will satisfy every age threshold, consent standard or advertising restriction. All policies deserve careful review against each region's definitions, age thresholds, consent requirements and restrictions on marketing, profiling and data transfers.

COMPLIANCE

A Field Guide to Privacy Law for Companies Entering the US Market

by Kevin Coy and Erin Doyle JULY 20, 2026

Businesses wanting to operate in the US have a variety of laws and regulations to consider

READ MORE

App-store age signals are an emerging compliance issue

App-store accountability laws create another compliance layer. Rather than leaving every developer solely responsible for building a separate age gate, these laws allocate responsibilities among app stores, operating-system providers and app developers.

With multiple laws already passed — and several laws that have been proposed — we are likely to see a patchwork that adds to the confusion. Some of these laws will place the core age-verification and parental-consent obligations on app stores while requiring developers to provide age ratings and notifications. Others will be more developer-facing. And to make matters more complicated, legal challenges will impact the timing and scope of the laws.

For example, Texas S.B. 2420 took effect after the Fifth Circuit stayed a preliminary injunction blocking the law. The law requires covered app stores to verify users' age categories, associate minor accounts with parent accounts and obtain parental consent in specified circumstances. App stores must also make age-category and consent information available to developers. Developers in turn must assign age ratings, respond to significant changes and use the information consistently with the law's restrictions.

To make matters more complicated for app developers, app stores may have their own requirements.

Compliance requires more than a privacy-notice update

Companies should begin to mitigate risk in handling minors' data by determining whether they are collecting any data within the scope of any of these laws, which may not be as simple as whether they are collecting just age data. Companies then need to assess the value of that data, what kinds of compliance obligations may need to be met and what kind of operational changes may need to be made. Vendor contracts, analytics tools and advertising technologies should also be reviewed to confirm that minors' information is not transmitted in ways that conflict with the company's policy or applicable law.

Ballard Spahr summer associate T'Phani Perley-Schiele contributed to this report.

Tags: Data Governance

Previous Post

Telling Moments Compliance Leaders May Overlook in Investigations

Greg Szewczyk and Madison Etherington

Greg Szewczyk is a partner and practice leader of the privacy and data security group at law firm Ballard Spahr. He advises on complying with the ever-expanding patchwork of state, federal and international privacy and data security laws, including matters involving AI, vendor management and children's and teens' privacy compliance.

Madison Etherington is an associate in the privacy and data security group at law firm Ballard Spahr. She focuses her practice on privacy and data security matters, including compliance with state and federal data privacy laws like GDPR, CCPA/CPRA and TCPA.

Related Posts

Activist Investors Significantly Increase M&A Sale Pushes

by Staff and Wire Reports JULY 30, 2026

Massive data security confidence comes with high data security concerns.

Data Privacy Rules Built for Human Behavior Have an AI Agent Problem

by Srikanth Sallaka JUNE 8, 2026

Regulators are beginning to treat under-governed AI deployments as intentional conduct

Surveillance Pricing: You're Watching Consumers — and Government Is Watching You

by Kwamina Williford, Christopher J. Armstrong, Ashley Joyner Chavous and Benjamin Genn
MAY 22, 2026

Practices that rely on consumer data or opaque pricing mechanics are increasingly evaluated through a consumer protection and data governance...

SOC 2 Is Broken. The Delve Scandal Is Showing Us How.

by Clarence Chio MAY 21, 2026

Report published by the DeepDelver group shows just how thin the SOC 2 chain of trust can become under pressure

oin the conversation

t the week's top news, opinion and events -- right to your inbox!

ail*

ne*

ne*

untry*

Please Select

at's your current role?*

Please Select

I is committed to protecting and respecting your privacy. We will send you our weekly wsletter as requested, and from time to time, may also send you carefully screened information out webinars and downloads.

I agree. I know I can unsubscribe anytime.*

I agree to allow CCI to store and process my personal data in accordance with the privacy policy. *

Submit


LRN WEBINAR SERIES
From pilots to production -
Governing AI that's already in your organization
Watch the Webinar
AI
LRN Inspiring Principled Performance


2026 UPDATE
Getting Governance Right
2026
From leading experts, 14 essential reads for boards navigating an era of heightened expectations
Effective governance is no accident
DOWNLOAD


traliant
Preventing Workplace Harassment
Now a Cinematic Training Experience
Preview the course

Search...

rivacy Policy | AI Policy

*ounded in 2010, CCI is the web's premier global **independent** news source for ompliance, ethics, risk and information security.*

ot a news tip? Get in touch. Want a weekly round-up in your inbox? Sign up for free. No ubscription fees, no paywalls.

ollow Us

Browse Topics:

CCI Press
Compliance
Compliance Podcasts
Cybersecurity
Data Privacy
EBooks Published By CCI
Ethics
FCPA
Featured
Financial Services
Fraud
Governance
GRC Vendor News
HR Compliance
Internal Audit
Leadership And Career
On Demand Webinars
Opinion
Research
Resource Library
Risk
Uncategorized
Videos
Webinars
Well-Being
Whitepapers