KPMG

Regulatory Alert

Regulatory Insights

June 2025

Focus on Children's Online Privacy Protections

KPMG Regulatory Insights:

- ***Personal Information:*** *Changes in the collection, data, use and retention of children's personal information, including biometric identifiers.*
- ***Data Security and Retention:*** *Heightened standards to show 'reasonable need' for use/retention and security based on data sensitivity.*
- ***Burden on Providers:*** *Focus on parental consent, but also a shift of burden from parents to providers for safety/security.*
- ***States Step In:*** *State laws and regulations can diverge from (and may expand on) federal requirements in areas such as the definition of "child", covered operators, and parental controls.*

Amid the ongoing push for U.S. leadership in technology innovation and heightened attention to AI, cybersecurity, and data protection, federal regulators and individual states are looking to strengthen privacy protections for children's personal information. Examples include:

1. A Federal Trade Commission (FTC) workshop examining children's online safety
2. Amendments to FTC regulations implementing the Children's Online Privacy Protection Act (COPPA)
3. Recent state laws and regulations covering protections such as parental consent, disclosure, and data retention

FTC Workshop

On June 4, 2025, the FTC conducted a public workshop to bring together "parents, child safety experts, and government leaders" to examine concerns related to children's online protections, including "addictive design features," parental authority, and exposure to "harmful content" as well as to discuss potential solutions, including age verification and parental consent requirements.

Key topics included:

- Use of FTC's consumer protection scope to enforce age verification and children's privacy
- Stronger requirements for operators to seek parental consent regarding users under the age of 13
- Balancing protecting children's data against competitive entrepreneurialism
- Use of incentives before penalties for media companies to strengthen age verification
- Partnership between the states and parents to shield children from harmful content online, as opposed to sole responsibility belonging to parents
- Legislative efforts to increase children's online privacy protections, such as the recently enacted Take It Down Act and other bills under consideration (e.g., COPPA 2.0, Kids Online Security Act (KOSA), App Store Accountability Act), including provisions on:
  - Minimization of data gathering from children
  - Algorithmic transparency for sites directed at children, including mixed audience sites
  - Increasing focus on state-level legislation for age verification
- Gaps in regulation for teenagers (users between the ages of 13 and 18), including parental rights to delete children's data

- Segregation of data for minors on separate servers from aggregated data for adult users
- Educational plans for teaching privacy and online safety to children

Amendments to the FTC COPPA Rule

The FTC finalized amendments to update its rule implementing the Children's Online Privacy Protection Act (COPPA), which requires websites and online services to obtain verifiable parental consent before collecting, using, or disclosing the personal information of children under 13 years of age. The final amendments are generally the same as previously proposed (read the KPMG Regulatory Alert), though provisions related to education technology and the role of schools were deferred in anticipation of future rulemaking by the Department of Education under the Family Educational Rights and Privacy Act (FERPA).

The amendments become effective June 23, 2025, with compliance required by April 22, 2026 (though certain provisions related to COPPA Safe Harbor Programs have earlier compliance dates (e.g., 90 days and six months after publication of the final rule.))

The amendments include:

Topic	Description
Definition of "Personal Information"	Expanded to include government-issued identifiers and biometric identifiers such as fingerprints, handprints, retina and iris patterns, DNA sequences, voiceprints, and gait patterns. Exception from prior parental consent provided for collection of audio files containing a child's voice and no other personal information for purposes of responding to a request.
Third-Party Data Sharing	Requirement for separate parental consent before disclosing children's personal information to third-party companies for targeted advertising or other purposes.
Data Security Programs	Requirement for operators to establish, implement, and maintain a written information security program to protect personal information. No need for a separate policy for children's data if an existing policy meets the requirements.
Data Retention/Deletion	Requirement for operators to retain personal information collected from children only for as long as necessary to fulfill the original purpose for collecting it; data may not be retained indefinitely. A written data retention policy must set forth the purposes for which the information is collected, the business purpose for retaining it, and the timeframe for deleting it.
Parental Consent	New methods to obtain verifiable parental consent, including: — Text messages paired with additional verification steps (in certain conditions) — Knowledge-based authentication (e.g., questions) — Facial identification matches with government-IDs
Mixed-Audience Sites	Definition of mixed-audience to include sites: — Directed to children but not targeting children as primary audience. — Do not collect personal information before determining if the visitor is a child. Retention of the "two-step" process for determining a "mixed audience" site. Parental consent exceptions apply to mixed audience sites.
Age-Gating	Mixed audience sites and services may collect personal information for the limited purposes of determining visitor age. Age-gating (asking user for their age) must not default to a set age or encourage falsification of age information.
Safe Harbor Program	Program participants must publicly disclose membership lists. Enhanced reporting to the FTC, including an independent assessment of compliance with the program guidelines, a description of the business model, consumer complaints received, and disciplinary actions taken.

State Laws and Regulations

States are actively introducing laws and regulations to protect children (up to 13 years of age) and minors/teens (13-17 years of age) and their personal information on social media, gaming platforms, and other digital services. These protections vary by state and may include:

Topic	Description
Parental Consent and Age Thresholds	Verifiable parental consent required for online activity of children between the ages of 13 and 17 (age thresholds vary by state), including: — Collection and use of data — Push feeds and notifications — Unsolicited direct messaging — Targeted advertising, algorithmic recommendations More than 20 states have implemented identity verification protections (e.g., AL, KS, TN, VA).
Notice and Data Management	Standards for use of children's data, including age-appropriate and concise notices and detailed transparency about ads and data handling practices (e.g., IL). Requirements around retaining children's data, including data minimization, retention, and prompt deletion, limiting data collection to what is necessary and requiring deletion once the data are no longer needed (e.g., OH).
Enforcement	Enforcement mechanisms for violations of children's privacy laws, e.g., laws in FL, IL, NY, VA authorize civil penalties.

For more information, please contact Amy Matsuo or Orson Lucas

Contact the author:

Amy Matsuo
Principal and National Leader
Regulatory Insights
amatsuo@kpmg.com