PUBLICATION

Impact on Companies with Online Services as Children's Data Protection Gains Ground in Colorado

Authors: Vivien F. Peaden
August 11, 2025

Companies offering online services take heed: effective October 1, 2025, Colorado's new children's data protection framework is sending a clear signal of where the future of privacy and social media regulation is headed across the U.S.

Enacted only four years ago, the **Colorado Privacy Act** (CPA) may still be in its early years, but it has quickly earned a reputation as **a trendsetter in children's and teen privacy regulation**. On July 29, 2025, the Colorado Department of Law proposed an amendment to the regulations implementing the CPA (CPA Rules) to enhance data protection for individuals under 18. **Beginning on October 1, 2025**, the CPA, as amended under the Senate Bill 24-041, will impose additional compliance obligations, including a duty of reasonable care to avoid heightened risks of harm to children and teenagers. Notably, these enhanced children's data protection obligations apply to all companies offering online services, products, or features to Colorado residents, **irrespective of their revenue or the volume of data they process.** The amended CPA is expected to have wide-reaching impact on businesses operating in the digital space across sectors, from social media, e-commerce, AdTech, and EdTech to health and wellness platforms.

Key Definitions:

Effective October 1, 2025, the amended CPA expands its scope to cover any business that provides goods, services, or content through online platforms, mobile applications, and other digital channels to Colorado consumers under 18 (**Minors**). Notably, the new CPA requirements apply regardless of the volume of data processed or revenue derived from such activities, broadening the law's reach beyond the thresholds that typically trigger general CPA obligations.

- **Minor**: Any consumer under 18 years of age.
- **Online Service, Product, or Feature (Online Services)**: Any service, product, or feature that is provided online, with a few exceptions.
- **Heightened Risk of Harm to Minors**: Data processing that poses a reasonably foreseeable risk of causing Minors unfair or deceptive treatment; financial, physical, or reputational injury; or unlawful intrusion of privacy.

What's New:

1. **Knowledge Standard**: The draft CPA Rules seek to define when a business that determines how and why personal data is processed (the "**Controller**") and offers Online Services "Knows or Willfully Disregards" that a consumer is a Minor. Specifically, the Colorado Department of Law's proposal considers the following factors:

- Direct Disclosure: A Controller directly receives information from a parent or consumer indicating that the consumer is a Minor.

- Minor-Oriented Design or Activities: A Controller's website or service specifically appeals to Minors based on subject matter, visual content, language, and use of Minor-oriented activities and incentives.
- Age-Based Categorizations and Marketing: A Controller uses user-generated content or other data to categorize a consumer as a Minor for marketing, advertising, or internal business purposes.

2. **Minor-Oriented System Design**: The amended CPA restricts a Controller from using **any system-designed feature to significantly increase, sustain, or extend a Minor's use of the online services** (**Minor-Oriented Feature**). Under the draft CPA Rules released on July 29, 2025, the Colorado Department of Law considers the following factors:

- Purpose: The system design is developed to significantly increase, sustain, or extend a Minor's use of or engagement with the service.
- Actual Impact: The online feature has been shown to boost user engagement beyond what is reasonable for similar services.
- Addictive or Harmful Effects: The design contributes to addictiveness or causes harm to Minors in the context in which it is used.

3. **Valid Consent**: Beginning on October 1, 2025, a Controller shall not deploy the Minor-Oriented features described above unless prior, affirmative consent is obtained:

- Children under 13: A Controller must obtain verifiable parental or guardian consent (compliance with COPPA suffices).
- Children over 13 and under 18: A Controller must obtain the Minor's own consent.

Under the amended CPA, valid consent must be a clear, affirmative action and cannot be obtained through manipulative mechanisms. Significantly, the draft CPA Rule provides that if a Minor-Oriented feature is off by default but toggled on by the Minor, that act is considered valid consent.

Who Should Pay Attention

The amended CPA will impact a wide range of companies that offer goods, services, or content through online platforms to Colorado residents under 18, including the following:

- **Tech and Online Services**: Social media, gaming, streaming, and online marketplaces that are likely used by Minors.
- **EdTech and Educational Platforms**: Online learning tools and student engagement services, especially those used by K-12 students.
- **Media and Content Providers**: Companies producing or distributing digital content likely to be accessed by Minors.
- **Retail and E-Commerce**: Online retailers and marketplaces where Minors can create accounts or make purchases.
- **Ad Tech and Marketing Analytics Firms**: Firms involved in behavioral advertising, profiling, or audience segmentation that may include Minors.
- **Health and Wellness Apps**: Platforms collecting health, fitness, or wellness data from Minors.
- **Location-Based Services**: Apps and services that collect or process precise geolocation data from Minors.

What a Controller Must Do on or After October 1, 2025

With October 1, 2025, fast approaching, companies that provide Online Services should:

1. Evaluate **Minor-Oriented features**: Unless proper consent is obtained, a Controller is prohibited from:

- processing a Minor's data for targeted advertising, selling a Minor's personal data, or profiling with significant effects;
- using Minor's personal data for purposes other than those disclosed at collection or for longer than necessary;
- deploying Minor-Oriented Features; or
- collecting precise geolocation data except when necessary to provide the service, and only for the required duration.

2. **Conduct Data Protection Assessments**: For any Online Services that present a heightened risk of harm to Minors, companies must conduct and periodically review a data protection assessment and retain documentation for at least three years after processing ends.
3. **Streamline Consent Workflows**: Companies should ensure that consent is obtained through a clear, affirmative action, particularly where system design features could increase a Minor's engagement. For users under 13, workflows must include mechanisms to obtain verifiable parental consent in compliance with applicable law.
4. **Review Privacy Notices, Terms of Use, and Internal Policies to Reflect These Changes**: Specifically, a Controller shall take reasonable steps to mitigate heightened risks of harm to Minors, including risks of unfair treatment, injury, unauthorized disclosure, or offensive privacy intrusions.

Summary:

Colorado's amendment to its comprehensive privacy laws reflects a growing trend across the United States: states are taking strong steps to safeguard children's data in an increasingly digital world. As Minors spend more time online, **states are stepping in** to fill the gaps left by outdated federal laws. More than a dozen states have passed laws that address Minor's data protection, online activities, and social media addictions, including Vermont (passed in 2025), Maryland (enacted in 2024), and Nebraska (enacted in May of 2025). Colorado's approach focuses on limiting data collection, regulating Minor-Oriented design features, and mandating parental consent, verification, and disclosure requirements for high-risk online data collection. For companies offering Online Services, Colorado's framework is both a **compliance obligation and a clear signal** of where the future of children's data regulations is headed across the U.S.

If you have any questions or would like to discuss this topic, please reach out to Vivien F. Peaden, AIGP, CIPP/US, CIPP/E, CIPM, PLS, or any member ofBaker Donelson's Data Protection, Privacy and Cybersecurity Team.