September 9, 2025

The Honorable Phil Weiser
1300 Broadway St.
Denver, CO 80203

Re: Requests for Input on Rules Governing Children's Online Data Amendments

Dear Attorney General Weiser:

The Computer & Communications Industry Association (CCIA) is pleased to respond to the Colorado Office of the Attorney General (OAG)'s request for input on the Colorado Privacy Act (CPA) rules governing children's online data amendments ("the proposed Rules").[1] As the OAG weighs potential modifications to the proposed Rules, CCIA offers the following proposals to guide deliberation:

Rule 6.13.A.1.c – Duty Regarding Minor Data – Knowledge Standard

This example should be removed. Though well-intentioned, it can enable malicious actors to file false reports and label adult users as minors, or file reports on children with whom they have no legal relationship. Controllers should not be subject to liability in these situations. For these reasons, best practices allow minors to report on their own safety concerns, rather than allowing parents and guardians to assume control of this process. For example, the European Commission's Digital Services Act guidance states that controllers should "Ensure that reporting, feedback and complaints are confidential and anonymous by default, while providing the option for *minors* to remove anonymity."[2]

Rule 6.13.A.2 – Duty Regarding Minor Data – Knowledge Standard

The Children's Online Privacy Protection Act (COPPA) rules specifically define what constitutes a "Website or online service directed to children."[3] The proposed rules should align with federal law by adopting COPPA's standards for when a user is "directed to" an online service, and then replacing all references to children with "Minors." Additionally, CCIA recommends a grace period to allow controllers time to update their practices after this rule is instituted.

---

[1] CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy.

[2] *Approval of the content on a draft Communication from the Commission - Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065* § 77.d (2025), *available at* https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors (emphasis added).

[3] *See* Children's Online Privacy Protection Rule (COPPA Rule), 16 C.F.R. § 312.2 (2025), https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312.

Rule 6.13.A.2.a – Duty Regarding Minor Data – Knowledge Standard

This rule lists circumstances where "A Controller creates and distributes marketing and promotional materials related to the website or service that specifically appeal to Minors" as an example of controllers directing websites or services to minors. This example risks encompassing controllers who design products and services to appeal to younger adults, but whose appeal also extends to older minors. To reduce such risk, this example should be limited to controllers who *intentionally* create and distribute such promotional materials, and should only extend to marketing and promotional materials that explicitly mention appeal to minors.

Rule 6.13.A.3 – Duty Regarding Minor Data – Knowledge Standard

This rule does not account for the rare cases in which controllers receive one piece of information indicating that a user is a minor, and another piece of information indicating that the same user is an adult. If, for instance, a user enters a 2005 birth date when signing up for an online service and a 2009 birth date when signing up for another service offered by the same controller, either birth date could have been mistakenly entered. Classifying the user as a minor would best protect the user's privacy, yet this rule incentivizes controllers to classify the user as an adult to avoid a finding of willful disregard. This rule should be amended so that controllers are not penalized for adopting the safest course in such situations.

Rule 6.14.A – Duty Regarding Minor Data – System Design Features

As CCIA noted in its July comments on the proposed Rules, CCIA advocates limiting this rule's scope to cases where (1) a system design feature uses deceptive and/or misleading means to increase time spent using the product, service, or feature; (2) the design feature harms consumers; and (3) restricting use of the system design feature would not infringe on freedom of expression.[4] The Supreme Court has held that system design features constitute protected free expression: In 2023, the Court held in *303 Creative LLC v. Elenis* that "The First Amendment prohibits Colorado from forcing a website designer to create expressive designs speaking messages with which the designer disagrees."[5] In 2024, it held in *Moody v. NetChoice LLC* that "The government may not, in supposed pursuit of better expressive balance, alter a private speaker's own editorial choices about the mix of speech it wants to convey."[6] Without the above limitation, this rule risks encompassing many forms of protected speech, including online books, music, news, and educational resources.

Rule 6.14.A.1 – Duty Regarding Minor Data – System Design Features

This rule does not adequately distinguish design choices that are deceptive and misleading from those that merely create content that their consumers enjoy. Online services that design their systems to enhance users' experiences will inherently increase user engagement even

[4] *CCIA Comments Re: Requests for Input on Rules Governing Children's Online Data Amendments* (July 10, 2025), at 2, https://ccianet.org/library/ccia-written-comments-on-the-colorado-privacy-act-childrens-privacy-rulemaking-process/.
[5] 143 S. Ct. 2298, 2303 (2023).
[6] 144 S. Ct. 2383, 2403 (2024).

when they do not use any deceptive or misleading features. However, this rule appears to equate controllers who merely wish to design better products with those who employ deceptive practices: both types of controllers develop system design features "in order to significantly increase, sustain, or extend a Minor's use of or engagement with an online service, product or feature." In fact, since better safety features can "significantly increase, sustain, or extend" use of an online service, the rule as written risks disincentivizing the addition of privacy and security enhancements. To avoid this, the rule should be limited to controllers who use deceptive or misleading systems.

Rule 6.14.A.2 – Duty Regarding Minor Data – System Design Features

This rule requires clearer guidance if it is to be applied consistently and objectively. It is unclear when a system design feature has "been shown to increase use or engagement beyond what is reasonably expected." This rule should specify what standards will be used to make such assessments, and what types of evidence can be considered when making them.

Rule 6.14.A.3 – Duty Regarding Minor Data – System Design Features

The term "addictiveness" lacks a definite scientific meaning. Humans engage in various compulsive and repetitive behaviors — some of which may negatively impact physical and/or mental health. These could range from binge eating unhealthy foods to exercising excessively to watching favorite shows for hours on end. However, these behaviors do not necessarily amount to "addictions". The most recent edition of the *Diagnostic and Statistical Manual of Mental Disorders: Fifth Edition Text Revision (DSM-5-TR)* declined to include definitions for "Internet gaming disorder," "Internet addiction," "excessive use of the Internet," or "excessive use of social media," noting that "[g]ambling disorder is currently the only non-substance-related disorder included in the *DSM-5-TR* chapter 'Substance-Related and Addictive Disorders.'"[7] CCIA therefore recommends changing this rule to "Whether the system design feature has been shown to harm Minors when deployed in the specific context offered by the controller."

Rules 6.14.B.1-2 – Duty Regarding Minor Data – System Design Features

Defining "media" more specifically would be useful. If "media" is interpreted broadly, these rules risk barring online shopping websites from offering personalized recommendations to customers or advertising their products. This risk can be avoided by clarifying that offering personalized recommendations and first-party advertising are "necessary to the core functionality of an online service, product or feature" for online sellers under rule 6.14.B.3, and are thus exempt from the requirements in rules 6.14.B.1-2.

Additionally, these rules should allow controllers to base personalized recommendations on general inferences about overlapping consumer preferences: If a minor buys one book on a particular topic, the seller can justifiably recommend other books on the same topic by different authors, even if the minor never searched for them. The seller can make this recommendation without any "other information associated with the Minor or the Minor's

[7] Am. Psychiatric Ass'n, *Diagnostic and Statistical Manual of Mental Disorders: Fifth Edition Text Revision* (2022).

device" — if the seller knows that readers of the first book are disproportionately likely to buy the second, it can offer such recommendations without any detriment to their customer's privacy. Moreover, as CCIA noted in its July comments, personalized recommendations "help screen out age-inappropriate content, and are a useful bulwark against the proliferation of unwanted content like spam."[8] The rules should specify directly that controllers are allowed to make such recommendations.

Rule 6.14.B.4 – Duty Regarding Minor Data – System Design Features

This rule should allow the same personalized recommendations discussed above: A controller can use general inferences about consumer preferences to make personalized recommendations without collecting any information that jeopardizes minors' privacy. As written, however, controllers might be unable to make such recommendations even if they are solely based on prior usage of their own products and services. Any recommendation made on a minor's account page could be said to be "persistently associated with the Minor or the Minor's device." Moreover, many basic features of online services will not work correctly without collecting some minimal information about a user's device, such as determining a user's country to set a default language. To avoid this problem, CCIA recommends specifying that such personalized recommendations are "necessary to the core functionality of an online service, product or feature" for online sellers under rule 6.14.B.3, as above.

Rule 6.14.B.6 – Duty Regarding Minor Data – System Design Features

CCIA recommends adding more examples of specific "countervailing measures" that would meet this exception's criteria, such as parental controls and website features that are turned off by default.

Rule 7.03.B.3 – Requirements for Valid Consent

CCIA welcomes this rule, but recommends extending it to cases where a minor's parent or guardian turns on the feature in question. Controllers should be able to treat a parent's decision to turn on a feature that is off by default as affirmative consent, just as they can for minors.

Additionally, the Colorado Privacy Act lists "Data maintained by a state institution of higher education… for noncommercial purposes" among the exceptions to controller obligations. CCIA suggests clarifying that this exception also applies to this rule.

* * * * *

We appreciate the OAG's consideration of these comments. CCIA looks forward to continuing to participate in the OAG's ongoing regulatory process, including reviewing and providing feedback on the series of proposed Rules. We hope the OAG will consider CCIA a resource as these discussions progress.

Sincerely,

[8] *CCIA Comments*, *supra* note 4, at 1.

Aodhan Downey
Regional State Policy Manager, West
Computer & Communications Industry Association