



October 2, 2026

Vermont Office of Attorney General
109 State Street
Montpelier, VT 05609-1001

RE: Vermont Age-Appropriate Design Code Rulemaking

Dear Attorney General Clark,

Thank you for your ongoing consideration of input concerning the Vermont Age-Appropriate Design Code (AADC). The Future of Privacy Forum (FPF) writes to provide perspectives focused on (1) prohibited data and design practices; (2) personalization and compulsive use; and (3) age assurance. We offer several considerations and recommendations intended to strengthen the proposed regulations by reducing ambiguity and supporting interoperability between the proposed rules with those in other leading U.S. privacy and online safety regulatory regimes where practicable, including:

1. Clarifying that certain administrative and technical functions are “necessary to provide a service”;
2. Aligning secondary use requirements with existing privacy laws;
3. Clarifying rules and restrictions related to online service personalization to preserve necessary or beneficial practices;
4. Clarifying rules on compulsive use by providing metrics for what constitutes unacceptable engagement;
5. Clarifying that graduated escalation is a factor for businesses to consider when selecting appropriate methods under the rule;
6. Defining clear technical thresholds or standards to assess what constitutes a “material risk of misclassification”; and
7. Consulting comparable state agency rulemaking processes for age assurance when considering adjustments or clarifications to the proposed rule.

FPF is a non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies. FPF seeks to support balanced, informed public policy and equip regulators with the resources and tools needed to craft effective regulation.¹

I. Prohibited Data and Design Practices

There is an ongoing trend in state privacy legislation—reflected in the Vermont AADC and these draft rules—towards substantive data minimization requirements that tie permissible collection and/or processing of personal data to what is necessary to provide a specifically requested product or service. FPF writes to identify several potential ambiguities and tensions in the proposed provisions on data minimization and secondary use.

¹ The opinions expressed herein do not necessarily reflect the views of FPF’s supporters or Advisory Board.

A. Consider clarifying that administrative and technical functions, such as preventing security incidents, are per se “necessary to provide a service.”

The Vermont-AADC provides that a covered business shall not “collect, sell, share, or retain any personal data of a covered minor that is not necessary to provide an online service, product, or feature with which the covered minor is actively and knowingly engaged.”² This is a “substantive data minimization” obligation because it establishes rules for the collection and/or processing of personal data that tie permissible processing to consumer expectations and the functionality of a given product or service.³ Similar requirements have been included in other state privacy laws, such as the Maryland Online Data Privacy Act (MODPA) and the New York Child Data Protection Act (NYCDPA).⁴

Substantive data minimization obligations such as these are written to recenter individuals’ expectations as the legal justification for the collection and use of personal data. However, the current requirements in the proposed rule are unusually strict. The proposed rule would define “necessary to provide a service” as processing of personal data that is “strictly required to provide a specific feature directly responsive to an express and unambiguous request by a covered minor and cannot reasonably be achieved through less data-intensive means.”⁵ The definition further provides that “[p]ersonal data use shall not be considered unnecessary solely because it supports security, fraud prevention, accessibility, or other functions reasonably undertaken in the best interests of covered minors and essential to the operation of the requested online service, product, or feature.”⁶

FPF recommends that the Office consider providing additional factors to determine “necessity,” providing businesses with more guidance as to permissible processing of covered minors’ personal data. Offering a digital service, product, or feature requires processing personal data for back-end technical and administrative purposes that, while not directly essential for offering a given product, service, or feature, nevertheless are vital for the business to function. The current definition of “necessary to provide a service” recognizes this by identifying the need to process personal data for security, fraud prevention, and accessibility. However, that exception could be revised to more affirmatively allow such other functions, especially when undertaken in the best interest of covered minors.

New York’s youth privacy law, the NYCDPA, provides an illustrative example of how to allow for such functions. That law allows a covered entity to process a minor’s personal data to the extent that doing so is strictly necessary for one of many enumerated permissible purposes, which include processing for internal business operations, identifying and repairing technical errors that impair functionality, protecting against malicious activity, and more.⁷ The Office should consider designating similar activities as “necessary to provide a service.”

² 9 Vt. Stat. Ann. § 2449f(a)(1).

³ See generally Jordan Francis, *Data Minimization’s Substantive Turn: Key Questions and Operational Challenges Posed by New State Privacy Legislation* (June 2025), <https://papers.ssrn.com/id=5309096>.

⁴ Md. Code Ann. Com. Law § 14–4707; N.Y. Gen. Bus. Law § 899-ff.

⁵ Proposed rule for § 2449f, at page 3.

⁶ *Id.*

⁷ N.Y. Gen. Bus. Law § 899-ff.

The draft rule could also provide covered businesses with additional flexibility by more explicitly tying the data minimization requirement to consumers' reasonable expectations. For example, Maryland has done this for MODPA. FAQs from the Maryland Attorney General's Office provide: "A business can determine what is 'reasonably necessary and proportionate to provide or maintain a specific product or service' based on the expectations of the reasonable consumer about how the data that is collected will be used."⁸

Other laws can provide additional guidance on when processing personal data is consistent with an individual's reasonable expectations. The California Consumer Privacy Act (CCPA) regulations provide that a business may only collect and process personal information for purposes that are consistent with consumers' reasonable expectations.⁹ Consumers' reasonable expectations, in turn, are based upon several factors: (1) the relationship between the consumer and the business; (2) the type, nature, and amount of personal information that the business plans to collect or process; (3) the source of the personal information and the business's method for collecting or processing it; (4) the specificity, explicitness, prominence, and clarity of disclosures to the consumers about the purpose for collecting or processing their personal information; and (5) the degree to which the involvement of service providers, contractors, third parties, or other entities in the collecting or processing of personal information is apparent to the consumer.¹⁰ The Office should consider adding comparable factors as part of the analysis for "necessity," to provide covered entities with more guidance.

FPF additionally recommends that, prior to finalizing the provisions on data minimization, the Office consult with other U.S. regulators who are tasked with enforcing similar substantive data minimization requirements, such as the New York Office of the Attorney General (NYOAG) and the Maryland Office of the Attorney General, to learn from their experience in enforcing their laws' requirements. The NYOAG went through a similar rulemaking process pursuant to the NYCDPA, and the resultant guidance on how to interpret that law's substantive data minimization obligations may prove useful.¹¹

B. For the purpose limitation requirements, consider aligning with existing privacy laws by allowing for secondary uses of previously collected data pursuant to consumers' consent or where the new purpose is compatible with the purpose at collection.

Purpose limitation provisions that limit secondary uses of personal data are a common feature of privacy and data protection frameworks. The proposed rule on prohibited data and design practices takes a strict approach to secondary use, prohibiting the use of a covered minor's personal data for any purpose other than the purpose for which it was collected. This is an unusually strict approach to secondary use, and FPF recommends that the Office consider making this rule more flexible, either by allowing secondary uses pursuant to meaningful opt-in consent by the individual and/or where the secondary use is compatible with the purpose for which the personal data was collected.

⁸ Maryland Off. Att'y Gen., Data Privacy in Maryland, <https://oag.maryland.gov/resources-info/Pages/data-privacy.aspx> (last visited Sept. 29, 2026).

⁹ Cal. Code Reg. tit. 11, § 7002.

¹⁰ *Id.*

¹¹ Off. of the N.Y. Att'y Gen., *New York Child Data Protection Act Implementation Guidance*, <https://ag.ny.gov/child-data-protection-act-guidance> (last visited Sept. 21, 2026).

Prohibiting secondary uses of personal data, with no qualifiers about the compatibility of the new use with the original purpose, is an inflexible approach that is not risk proportionate. As a practical matter, the proposed rules include a number of meaningful protections that would limit unexpected secondary uses of personal data even without this specific prohibition. For example, the proposed age assurance requirements include two distinct prohibitions on secondary use, providing first that “[a] covered business shall not: . . . use age assurance data for any secondary purpose,” and secondly that “[a] covered business shall not use age assurance data for any purpose other than determining whether a user is a covered minor or complying with obligations under this Rule.”¹² The substantive data minimization requirements also provide significant protections against unexpected secondary uses of personal data by prohibiting businesses from collecting, retaining, using, selling, or sharing personal data of a covered minor unless “strictly required to provide a specific feature directly responsive to an express and unambiguous request by a covered minor.”¹³

The proposed restriction is also in tension with the proposed rule’s own definition of “secondary use,” which is defined as “any use not necessary to provide the service or not reasonably expected by a covered minor, which includes profiling, recommendations, cross-service use, advertising, and model training, and applies regardless of disclosure.”¹⁴ That definition is concerned solely with uses of personal data that would be outside of a covered minor’s reasonable expectations. The proposed secondary use rule, however, creates a much stricter requirement by prohibiting the use of personal data “for any purpose other than the purpose for which it was collected.”¹⁵

Privacy and data protection frameworks typically allow for secondary uses of previously collected personal data, either where the new processing purpose is compatible with the purpose for which the data was collected or where the individual consents to the secondary use. For example, Vermont’s recently enacted comprehensive privacy law, the Vermont Data Privacy and Online Surveillance Act (VDPOSA), provides that a controller shall “not process a consumer’s personal data for any material new purpose that is neither reasonably necessary to, nor compatible with, the purposes for which the data were [collected], unless the controller receives consent from the consumer.”¹⁶ Some states, such as California, Colorado, and Connecticut, have provided additional guidance on permissible secondary uses without obtaining consumer consent. Connecticut’s law, for example, provides five factors for determining whether a secondary use is compatible with the original purpose based on:

- (i) the consumer’s reasonable expectation regarding such personal data at the time such personal data were collected based on the purposes that were disclosed to the consumer . . .

¹² Proposed rule for § 2449f, at pages 7 and 8.

¹³ Proposed rule for § 2449f, at pages 3 and 4 (definition of “Necessary to provide a service” and the data minimization section).

¹⁴ Proposed rule for § 2449f, at page 3.

¹⁵ Proposed rule for § 2449f, at page 5. Limiting this to “the” purpose for which the data was collected is potentially narrower than the statutory limit of “a purpose for which the personal data was collected.” 9 Vt. Stat. Ann. § 2449f(a)(2).

¹⁶ Vermont Data Privacy and Online Surveillance Act (VDPOSA), S.71, 2025-26 Reg. Sess., (Vt. 2026), § 2415e(a)(2). A controller is required to limit the collection of personal data to what is “reasonably necessary and proportionate in relation to the purposes for which the data are processed, as disclosed to the consumer.” § 2415e(a)(1).

- (ii) the relationship that such new purpose bears to the purposes that were disclosed to the consumer . . .
- (iii) the impact that processing such personal data for such new purpose might have on the consumer,
- (iv) the relationship between the consumer and the controller and the context in which the personal data were collected, and
- (v) the existence of additional safeguards, including, but not limited to, encryption or pseudonymization, in processing such personal data for such new purpose.¹⁷

By limiting restrictions on secondary uses of personal data to uses that are materially different than the purpose for which the data was collected, privacy laws balance individuals' expectations about how their data will be used with organizations' need to process that data even as the relevant service, product, or feature evolves. Adding this kind of compatibility test to the proposed rule would add this kind of flexibility while still respecting covered minors' reasonable expectations about how their personal data will be used.

II. Personalization and Compulsive Use

There has been a discernible shift in online safety legislation towards restrictions on platform design, and the Vermont AADC reflects this trend in several key provisions. FPF writes to identify potential ambiguities, tensions, and unintended consequences in the proposed rules addressing personalization and compulsive use.

A. Consider clarifying rules related to online service personalization to allow necessary tailoring and enjoyable or beneficial experiences for minors.

Numerous provisions throughout § 2449f address covered businesses' personalization practices: data minimization rules prohibiting data use for tailoring or modifying "media, features, or a covered minor's experience"; secondary data use limitations preventing the use of inferences or preferences to tailor an online experience (with no option for a minor to provide consent for such purposes); restrictions on using personal data or behavioral data to "select, recommend, rank, order, prioritize, or sequence media" for a minor, including based on viewing behavior or interaction history; and anti-circumvention rules preventing covered businesses from using alternative designs and technical or operational means to achieve substantially similar effects as a prohibited practice.¹⁸ While FPF appreciates the Office's aim to curtail foreseeably harmful personalization practices, the broad, brightline framing of these provisions may overly restrict covered businesses' ability to implement flexible, risk-proportionate personalization practices that serve minors, improve user experiences, and achieve online safety goals.

Applying risk-based regulation to personalization requires understanding what personalization fundamentally is and the range of contexts it serves. Personalization is the process of using data about an individual to tailor or adapt content recommendations, interface functionality, and

¹⁷ Conn. Gen. Stat. § 42-520, as amended by section 9 of Public Act 25-113 (2025).

¹⁸ Proposed rule for § 2449f, at pages 4-7 and 9.

experiences within an online service to that specific individual.¹⁹ A service may be personalized based on express preferences, data provided by the user, or observed behavior.²⁰ While online service personalization has recently been more commonly associated with recommendation system design, the range of personalization functions extends far beyond that one practice. Other illustrative examples of personalization include—a platform using a user’s age to implement safety defaults; a service surfacing relevant content and resources based on a student’s preferred subject selections in an educational platform; or a search engine prioritizing relevant results for a user based on past history and location, like a frequently visited local restaurant website.²¹

Given the wide range of personalization contexts and use cases—some improving convenience, effectiveness, or basic service utility, whereas others are implemented primarily to drive excessive engagement or monetization—broad, bright-line restrictions risk diminishing the benefits online services provide to minors. Instead, more nuanced, flexible, and risk-proportionate personalization restrictions that take into account the range of mitigations available to reduce risks of harm to minors may be more effective in achieving the online safety goals of broadly applicable frameworks such as the Vermont AADC.²² Addressing a broad range of personalization practices through substantive regulations, such as this proposed rule, is a relatively nascent endeavor by state agencies, so there are not yet many comparative examples to draw upon in this process. However, other state governments that are or will soon be exploring similar rulemaking topics, such as California and Colorado, may serve as useful regulatory companions for consultation.²³ In the meantime, FPF recommends crafting rules that consider the following key questions when assessing the risk of personalization practices across implementation contexts:

- (1) What were the data sources;
- (2) What were the categories of data collected and used;
- (3) How was the data retained and processed;
- (4) What was the purpose of processing the users’ data within a given implementation context; and

¹⁹ Daniel Hales & Holly Hawkins, *Personalization and Youth Online: Assessing Benefits, Risks, and Safeguards* (Future of Privacy Forum, June 2026), <https://fpf.org/wp-content/uploads/2026/06/FPF-Youth-Personalization-Report.pdf>.

²⁰ *Id.* at 6

²¹ *Id.*

²² *Id.* Many mitigations are available to address risks of harm to minors related to personalization practices depending on the implementation context and potential harms, including alternative recommender system design; tools allowing control over personal data use, content filtering, and preference selection; and well-defined, consistent requirements related to data minimization, retention, and transparency.

²³ See e.g., Daniel Hales & Bailey Sanchez, *FPF Submits Comments to Inform Colorado Minor Privacy Protections Rulemaking Process*, Future of Privacy Forum (Sept. 25, 2025), <https://fpf.org/blog/fpf-submits-comments-to-inform-colorado-minor-privacy-protections-rulemaking-process/> (responsive to the [OAG rulemaking process](#)); Covered Platform Restrictions & e-Safety Commission, [AB 1709](#), 2026-2027 Reg. Sess., (Cal. 2026) (designating OAG rulemaking for addictive design features, which may involve consideration of personalization or other regulatory requirements of similar kind to this rulemaking).

- (5) What mitigations can be implemented to reduce foreseeable risks of harm from personalization practices?

B. Consider clarifying rules related to compulsive use to provide metrics for unacceptable engagement or prolonged use beyond reasonable expectation in a given context.

To provide covered businesses with clarity, the Office should consider identifying specific thresholds for determining whether a design feature or practice significantly increases engagement beyond reasonable expectations. The proposed rule deems several practices as compulsive use, including those that:

- (i) [rely] on engagement optimization techniques, including the use of personal data or behavioral signals to **increase** a covered minor's interaction;
- (ii) [are] designed or reasonably likely to **increase, prolong, or intensify** a covered minor's interaction with the online service, product, or feature . . .²⁴

The rule also identifies several factors that the Office may consider when determining if a practice leads to compulsive use, such as—

- (i) A covered minor's **increases** in time spent, frequency of use, or session length;
- (ii) A covered minor's repeated or habitual patterns of engagement; . . .or
- (iii) Whether engagement occurs in the absence of a covered minor's express and unambiguous request.²⁵

While we appreciate the intent to restrict harmful engagement practices, the proposed rule's broad standards may discourage services from improving products and user experiences—or leave covered businesses uncertain about when engagement is permissibly enjoyable versus unacceptably engaging—if such improvements merely increase or prolong use. The proposed rule uses unqualified terms such as “increase,” “prolong,” and “intensify” to describe the impact of impermissible design practices on minor users' interaction patterns. Without further guidance, these terms are quite broad and may capture a range of practices that may even be beneficial to users even if they increase overall service or feature use habits. For example, a website that updates the design of its platform to enhance the user experience and service functionality may increase overall use patterns over time if those changes improve navigability or utility. In another example, a minor may increase or prolong time spent on an adaptive learning platform that improves its suite of curriculum offerings by adding course-relevant quizzes at the end of tutoring lessons. In both of these examples, services are improving product functionality in ways that generally benefit minors, but could be captured and scrutinized by these proposed regulations without further guidance. As a result, the line between discouraged design practices, and beneficial practices that improve user experiences and promote healthy engagement may be ambiguous under the rules as written.

Compulsive use caused by system design features is becoming an increasingly common subject of scrutiny by laws and regulations, but implementation of these requirements across the U.S. is

²⁴ Proposed rule for § 2449f, at page 7. Emphasis added.

²⁵ *Id.* Emphasis added.

still relatively nascent and complicated by the careful constitutional boundaries of targeting online design choices and protected expressive content.²⁶ Consequently, there is not yet an established regulatory framework for distinguishing system design practices that lead to compulsive uses versus those that don't. However, the Colorado and California Attorneys General Offices have both considered similar questions regarding compulsive use and addictive design features, and may serve as beneficial consultation resources for the Office's current efforts.²⁷

Aside from working with other state regulators, we recommend that the Office consider creating narrowly tailored criteria or evidence-based thresholds for assessing compulsive use metrics to improve clarity around these requirements. Without further metrics or guidance, it may be difficult for stakeholders to reliably distinguish between system design features that are good and enjoyable for users, including covered minors, and system design features that reach the point of harmful conduct and impermissibly increase engagement beyond reasonable expectation. Establishing thresholds for excessively increased or prolonged use paired with criteria assessing specific and demonstrable harms to minors could offer greater clarity to stakeholders and contribute to more consistent and reliable policy outcomes.

III. Age Assurance

The proposed rule on Age Assurance Privacy outlines a graduated escalation approach in adopting age assurance methods which seemingly aims to reduce the use of intrusive age assurance processes or techniques. In determining the appropriate instances to implement moderate-intrusion and higher-intrusion age assurance methods, the proposed rule requires covered businesses to determine whether lower-intrusion age assurance processes or techniques do not meet a "necessary level of accuracy or confidence."²⁸ Additionally, the proposed rule aims to reduce the use of age assurance techniques and processes with high error rates for minors, but does not define a technical threshold to determine when there is a "material risk of misclassification of covered minors."²⁹ Taken together, the proposed rule may render age assurance requirements ambiguous for covered businesses, thereby creating compliance challenges.

FPF recommends the Office adjust the proposed age assurance approach to allow ample flexibility for covered businesses to maintain and explore complex combinations of age assurance methods by considering: (1) risk proportionate approaches in age assurance adoption, (2) the implementation of technical thresholds, and (3) rulemaking approaches in other states.

²⁶ See e.g., *303 Creative LLC v. Elenis*, 600 U.S. (2023); N.Y. Gen. Bus. Law §§ 1500–1508 (2025) (New York enacted the "Stop Addictive Feeds Exploitation (SAFE) For Kids Act" in June 2024 and goes into effect in January 2027 now that regulations have been finalized); *NetChoice LLC v. Bonta*, No. 25-146, slip op. (9th Cir. Sept. 9, 2025) (California passed a law in September 2024 regulating personalized feeds for minors – this law is currently the subject of active litigation); *Moody v. NetChoice, LLC*, 603 U.S. 707 (2024) (finding First Amendment protections for certain expressive curation activities by entities).

²⁷ See *supra* note 23.

²⁸ Proposed rule for § 2449g, at pages 4 and 5.

²⁹ Proposed rule for § 2449g, at page 5.

A. The Office should consider clarifying the role of successive or graduated escalation methods as a factor in age assurance selection to encourage business adoption of risk-proportionate approaches.

While the proposed rules seemingly aim to establish a risk-proportionate framework, the combination of requirements in the proposed rule may undercut that goal. Specifically, the interplay between (1) the proposed rule’s requirements concerning “age assurance selection,” which define criteria for covered businesses to implement proportionate methods according to risk, and (2) the graduated escalation requirements, which *mandate* that businesses implement multiple successive mechanisms from least- to highest-intrusive methodologies tied to undefined assurance thresholds, may lead to compliance ambiguity and prevent businesses from effectively establishing risk-proportionate and privacy-preserving age assurance schemes.³⁰ Clarifying the role of successive or graduated methods as a factor in business’s age assurance selection process to achieve proportionate implementation within defined risk-assurance levels, rather than explicitly requiring graduated escalation, may better serve the goals of these regulations.

For additional information on age assurance considerations, we recommend the office refer to FPF’s *Unpacking Age Assurance* infographic that covers methodologies, relative privacy/assurance tradeoffs, and key terms relevant to age assurance implementation.³¹ It also demonstrates implementation of risk-proportionate waterfall or graduated assurance schemes.

B. The Office should consider providing clear technical thresholds or standards to assess what constitutes a “material risk of misclassification” across contexts or risk-levels.

The proposed rule presents ambiguities around misclassification thresholds, with language addressing both “a **material risk** of misclassification of covered minors” and “processes or techniques that **disproportionately misclassify** certain covered minors or groups of covered minors.”³² Imprecise misclassification standards may complicate age assurance implementation across varying contexts, as they can introduce additional uncertainties about what techniques and processes businesses are prohibited from employing. States including New York, South Carolina, and Minnesota have enacted laws and regulations requiring technical thresholds dependent on specific age thresholds and implementation triggers.³³ While each states’ requirements differ in age thresholds, timelines, and scope, state approaches tend to offer covered businesses and platforms flexibility to adopt appropriate age assurance methods tied to clear and specific technical benchmarks. The technical thresholds noted in the following table may serve as comparative examples for the Office’s consideration of similar standards.

³⁰ Proposed rule for § 2449g, at pages 4 and 5.

³¹ Future of Privacy Forum, *Unpacking Age Assurance: Technologies and Tradeoffs* (Feb. 2026), <https://fpf.org/wp-content/uploads/2026/02/FPF-Age-Assurance-v2.0.pdf>.

³² Proposed rule for § 2449g, at pages 5-6. Emphasis added.

³³ See **Table 1**.

Table 1. Comparison of Accuracy Rate Threshold Requirements for Covered Businesses Between New York, South Carolina, and Minnesota Laws and Regulations

Key: underline = Technical thresholds or associated age ranges

Jurisdiction	Law/Regulation	Text
New York	SAFE for Kids Act (S7694A) Rule 700.1(b)	Defined accuracy minimum. The <i>accuracy minimum</i> is defined as: (1) a rate of false positives for an age assurance method that is equal to or less than the following: • <u>0.1% of minors ages 0 to 7;</u> • <u>1% of minors ages 8 to 13;</u> • <u>2% of minors ages 14 to 15;</u> • <u>8% of minors age 15;</u> • <u>15% of minors age 17</u> (2) a rate of detecting method circumvention for an age assurance method that meets or exceeds 98%. (Rule 700.1(b)).
South Carolina	Stop Harm from Addictive Social Media Act (H4591)	Implemented confidence score requirements to determine account holders over 15. • <i>Preliminary estimation:</i> If the covered social media platform can conclude with <u>80% confidence</u> that an account holder is <u>over 15 years old</u>, then the covered social media platform can treat the account holder to be other than a child. Otherwise, the account holder will be treated as a child. • <i>Estimate revision:</i> If the covered social media platform can conclude with <u>90% confidence</u> that an account holder is <u>over 15 years old</u>, then the covered social media platform can treat the account holder to be other than a child. Otherwise, the account holder will be treated as a child. (Sec. 39-5-920(A-B)).
Minnesota	Social Media Safety law (HF 4138)	Provided confidence score requirements to determine account holders 16 years or older. (This social media law adopts similar requirements seen in South Carolina.) • <i>For new account users who have been on the platform for at least 25 hours in a 6-month period:</i> If the covered social media platform is able to conclude with an <u>80% confidence score (or greater)</u> that the user is <u>16 years or older</u>, the user will not be considered a child. • <i>For new account users who have been on the platform for at least 50 hours in a 6-month</i>

		<i>period</i>: If the covered social media platform is able to conclude with a <u>90% confidence score (or greater)</u> that the user is <u>16 years or older</u>, the user will not be considered a child. • <i>For Biannual Age Estimation Updates</i>: If the platform can conclude with a <u>90% confidence score (or greater)</u> that the account holder is <u>16 years or older</u>, the user will not be considered a child. If neither requirements are met, the user will be treated as a child user. (§ 325M.40, Subd. 2(a-c)).
--	--	--

C. The Office may benefit from consulting comparable state agency rulemaking processes.

Similar to Vermont, a number of states are in the process of developing or finalizing age assurance regulations. This year, California and New York promulgated rules concerning their age assurance standards which can be used as points of reference:

- **New York:** In July, Attorney General James released the finalized rules for the SAFE for Kids Act. Beyond requiring the previously mentioned accuracy minimum benchmarks, the rules also provide guidance on acceptable approaches to determining when users are minors, granting covered operators flexible guidelines for implementing age assurance methods.³⁴
- **California:** In May, the California Department of Justice published rules concerning the Protecting Our Kids from Social Media Addiction Act that includes a non-exhaustive list of methodologies that are reasonable for age determination, requiring methods to be quantifiably testable and consistently measurable.³⁵ Unlike New York, California does not require covered operators to meet an "accuracy minimum," demonstrating another approach to providing flexible standards.
- **Colorado:** In August, the Colorado Department of Justice published proposed rules for the Chatbot Safety Act seeking to provide implementation guidance on the statute's age assurance requirements.³⁶ The proposed rules provide criteria guiding operators' assessment of methods that may be "commercially reasonable or generally accepted," while allowing flexibility for when and how different operators may achieve compliance.

Engaging with regulators in these jurisdictions may provide additional guidance to the Office when fine tuning these proposed rules for implementation.

³⁴ See *SAFE for Kids Act Implementing Rules*, Office of the New York Attorney General, <https://ag.ny.gov/safe-for-kids-act-final-rule#safe-for-kids-act>.

³⁵ See *Notice of Proposed Rulemaking, Protecting Our Kids from Social Media Addiction Act Regulations*, California Department of Justice (published May 15, 2026), <https://oag.ca.gov/system/files/media/sb976-proposed-rulemaking.pdf>.

³⁶ See *Colorado Automated Decision-Making Technology & Chatbot Safety Rulemaking*, (published August 11, 2026) <https://coag.gov/ai/>.

* * *

Thank you for this opportunity to provide comment on these proposed regulations. We welcome any further opportunities to provide resources or information to assist in this important effort.

Sincerely,

Daniel Hales
Policy Counsel, U.S. Legislation & Regulation
dhales@fpf.org

Jordan Francis
Senior Counsel, U.S. Legislation & Regulation
jfrancis@fpf.org

Carisma De Anda
Youth Policy Research Contractor
cdeanda@fpf.org